Universität Leipzig
Fakultät für Mathematik und Informatik
Institut für Informatik

Administrationsmöglichkeiten eines Client/Server-DV-Systems

Diplomarbeit

Lehrstuhl für Computersysteme
Prof. Dr. W. Spruth

Leipzig, 07. 04. 1999

vorgelegt von
Patrick Agsten

Inhaltsverzeichnis

Abbildungs- und Tabellenverzeichnis

Abbildungen

Tabellen

Ziel der Arbeit

Die vorliegende Arbeit wurde in Zusammenarbeit mit dem Unternehmen SBS GmbH & Co. OHG in dessen Auftrag angefertigt. Sie systematisiert und beschreibt Begriffe sowie verfügbare Werkzeuge zum Enterprise-IT-Management. Von Interesse war hauptsächlich, welche Möglichkeiten zur Verwaltung von großen IT-Systemen heute geboten werden. In diesem Sinne gibt die Arbeit einen Überblick über das Thema „Enterprise-IT-Management".

Durch die Entwicklung von hostbasierten zu Client/Server-basierten Systemen haben sich die Problemstellungen im Betrieb von IT-Systemen verlagert. Die Verwaltung erfolgt aber in den meisten Unternehmen noch nach den herkömmlichen Prinzipien. In der Arbeit werden Sichtweisen vorgestellt, die zu einer demgegenüber kostengünstigeren und effizienteren Verwaltung führen.

Auch die Beziehung der IT-Verwalter zu den Benutzern von IT-Systemen hat sich geändert. Durch Outsourcing wurde die IT-Verwaltung rechtlich selbständig. Mit den Benutzern der IT sind Serviceverträge geschlossen worden. Diese enthalten inzwischen klare Regelungen, welche Funktionen durch den IT-Dienstleister bereitzustellen sind und wie abgerechnet wird. Daraus ergeben sich neue Anforderungen an die IT-Verwaltung. Auch diesen muß mit neuen bzw. angepaßten Verwaltungskonzepten Rechnung getragen werden.

Das IT-System der SBS migriert zu WindowsNT, dem daher in der Arbeit besondere Aufmerksamkeit gewidmet wird. WindowsNT ist ein recht junges Netzwerkbetriebssystem mit großem Entwicklungspotential. Es harmoniert gut mit den Arbeitsplatzbetriebssystemen Windows 3.x, Windows9x und WindowsNT Workstation, die heute mehr als die Hälfte aller Arbeitsplatzrechner bedienen.

Die Arbeit gliedert sich in vier Abschnitte. Der erste Abschnitt stellt die wichtigsten existierenden und entstehenden Standards zur Verwaltung von IT-Systemen kurz vor und klassifiziert Werkzeuge und Administrationsstrategien.

Im zweiten Abschnitt wird am Beispiel der SBS GmbH & Co. OHG dargestellt, wie IT-Systeme heute verwaltet werden. Dabei werden zunächst die im Zusammenhang mit Enterprise-IT-Management

stehenden Begriffe geklärt, da ähnlich wie vor ein paar Jahren beim Schlagwort Multimedia eine Begriffsverwirrung herrscht. Gleichzeitig wird damit eine Zusammenstellung von wichtigen Begriffen und ihren Bedeutungen geschaffen, wie sie nur in der Herstellerliteratur und dort leider meist nicht vollständig zu finden ist. Die Definitionen werden mit der Beschreibung der tatsächlich bei der SBS durchgeführten Maßnahmen unterlegt.

Der dritte Abschnitt beschreibt eine mögliche Integration der vorher angesprochenen Managementdisziplinen. Dabei wird klar werden, daß die angestrebte Integration eine Veränderung der Administrationsstruktur, insbesondere der Authentifizierungs- und Sicherheitsstrategien nach sich ziehen kann. Aufgrund der hohen Komplexität des Themas ist eine vollständige Auflistung aller Vorteile und Nachteile nicht möglich. Statt dessen wird an typischen praxisorientierten Beispielen gezeigt, welche Vorteile in konkreten Einzelfällen zu erzielen sind.

Der vierte Abschnitt gibt einen Überblick über derzeit am Markt verfügbare Produkte zum Enterprise-IT-Management. Dabei werden einige wichtige Eigenschaften dieser Produkte diskutiert, die anhand administrativer Erfordernisse des Managements ausgewählt wurden. Auf eine Untersuchung des gesamten Funktionsumfanges der Produkte wurde verzichtet, da der Rahmen der Arbeit dadurch gesprengt würde. Außerdem sind die funktionellen Anforderungen zu stark an das konkrete IT-System gebunden, als daß ein pauschaler Vergleich gelingen könnte. Für Vergleiche der Funktionen gibt es spezialisierte Anbieter, die eine auf das konkrete Umfeld zugeschnittene Untersuchung vornehmen können.

1 Einführung

Das Wörterbuch der Encyclopeadia Britannica definiert Management als überlegte Anwendung von Möglichkeiten zur Erreichung eines Ziels [MW1]. Dabei müssen zwangsläufig alle Möglichkeiten geprüft und gegebenenfalls zur Anwendung gebracht werden. Außerdem ist es erforderlich, neben Werkzeugen, die zum Zeitpunkt des Tätigwerdens des Managers zum Einsatz kommen, auch solche Verfahren zu berücksichtigen, die Entscheidungshilfen bereitstellen, indem z. B. langfristige Entwicklungen dokumentiert werden.

1.1 Standards im IT-Management

Bei den Bemühungen, Netzwerke zu standardisieren, entstanden sog. Managementprotokolle. Zunächst nur für den Einsatz bei der Verwaltung von Netzwerkhardware geplant, werden sie heute für die Softwareverwaltung eingesetzt.[1] In den letzten Jahren gibt es auch Bemühungen, die Verwaltung des gesamten IT-Umfelds standardisierend zu erfassen, um Qualitätskriterien spezifizieren zu können. So sind grundlegende Maßnahmen bereits im Qualitätssicherungsstandard ISO/EN 9001 festgehalten. Ein weiterer zertifizierbarer Standard zum Systemmanagement ist die ISO/IEC 14001 [ISO1]. Abbildung 1 zeigt die wichtigsten ISO-Standards und ihre Zusammenhänge.

[1] Eines der später vorgestellten Produkte operiert nach Angaben des Herstellers vollständig auf einem solchen Netzwerkmanagementprotokoll.

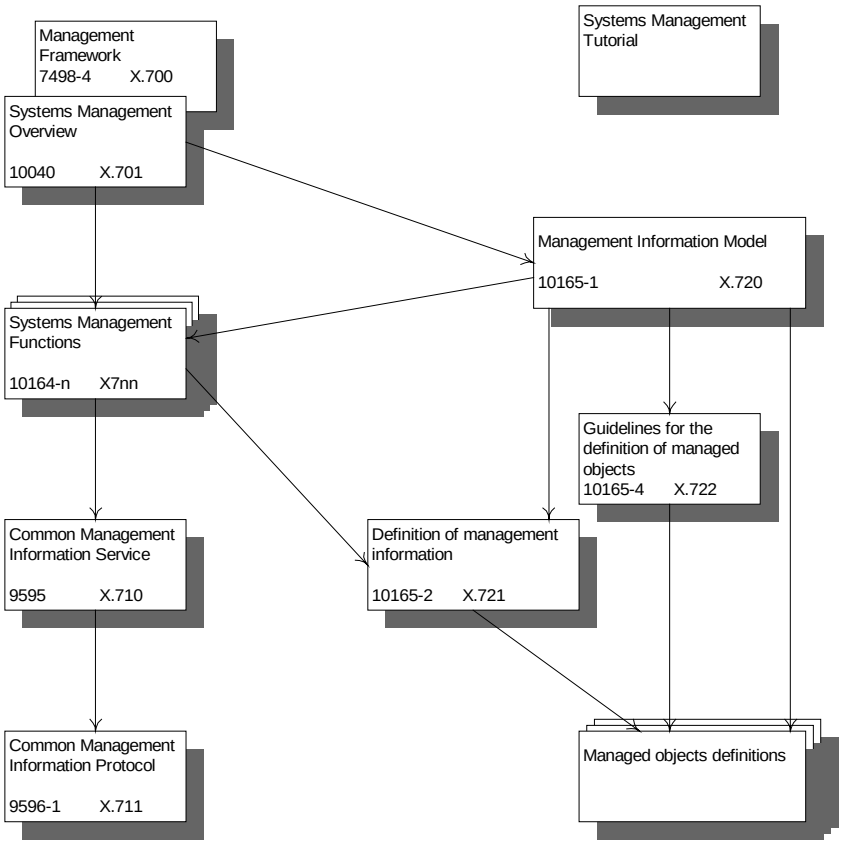

Abbildung 1: Zusammenhänge zwischen Standards [ISO2]

1.1.1 SNMP

SNMP (Simple Network Management Protocol) ist kein offizieller Standard. Es entstand an der Carnegie Mellon Universität [CMU1], als CMIP[2] in weiten Teilen noch nicht definiert war. Rein für TCP/IP entwickelt und für das Internet verwendet, wurde SNMP zum de facto Standard für Netzwerkmanagement. Einer der Gründe dafür ist, daß Hersteller von Netzwerkgeräten Code von Softwarehäusern verwenden konnten und damit teure Eigenentwicklungen vermieden [Held92]. Heute ist SNMP so stark verbreitet, daß kein Hardwarehersteller es

[2] Siehe Abschnitt 1.1.2

sich leisten könnte, Geräte ohne die entsprechende Unterstützung anzubieten.

Das Protokoll stellt eine Kommunikation zwischen einem Netzwerkmanagementsystem (NMS) und einem Netzwerkgerät her. Dazu ist es notwendig, daß auf dem NMS ein sog. Managerprogramm und auf dem zu steuernden Gerät ein sog. Agent laufen. Zwischen diesen werden die Informationen übertragen, die zur Steuerung des Netzwerkgerätes notwendig sind. SNMP ist allerdings allein nicht funktionsfähig. Es wirkt vielmehr mit sog. MIBs (Management Information Bases) zusammen, die ebenfalls an der Carnegie Mellon Universität definiert wurden [CMU4].

1.1.2 CMIP/CMOT

CMIP (Communications Management Information Protocol) ist ein ISO-Standard [ISO3], der ein Protokoll auf Anwendungsebene für den Austausch von Managementinformationen bereitstellt [Held92]. Ähnlich SNMP enthält es eine Reihe von Befehlen, die es Administratoren ermöglichen, auf entfernten Netzwerkkomponenten Lese- und Schreibvorgänge remote auszuführen. Während SNMP lediglich auf der Basis von TCP/IP arbeitet, ist CMIP fähig, auch andere Protokolle zu benutzen, da es auf dem OSI-Schichtenmodell [ISO4] basiert.[3] Auch die von CMIP verwendete Management Information Base zeichnet sich durch eine höhere Universalität aus. Die Objekte werden durch eine objektorientierte Sprache, ASN.1 (Abstract Syntax Notation One), angesteuert, die in OSIs *Guidelines for the Definition of Managed Objects* [ISO5] definiert ist.

Falls CMIP auf TCP/IP implementiert ist, lautet die Abkürzung CMOT (Communications Management over TCP/IP). CMIP/CMOT erreicht aus verschiedenen Gründen, die auf Fehler bei der Entwicklung des Standards zurückzuführen sind, nicht die Akzeptanz von SNMP [Rose94].

---

[3] Das OSI-Schichtenmodell ist hinreichend beschrieben, unter anderem bei Gilbert Held, und wird daher nicht näher erläutert.

1.1.3 RMON/RMON2

RMON (Remote Monitoring) ist eine Erweiterung von SNMP. Ziel war es, die Abfrage und Steuerung von *Remote Network Monitoring Devices*, worunter Monitore und Probes[4] verstanden werden, zu ermöglichen. Anders als bei SNMP, wo die Steuerung von aktiven Netzwerkkomponenten im Vordergrund stand, liegen die Ziele von RMON eher im Management des Netzwerkes und der Problemdiagnose. Konkret handelt es sich um Offline-/Online-Aufzeichnung von Arbeitsparametern, proaktives Monitoring, Problemerkennung und –meldung sowie verteilte Operabilität [CMU3][5]. RMON2 ist die aktuelle Version der RMON-Definitionen.

1.1.4 WBEM

WBEM (Web Based Enterprise Management) ist eine Entwicklung neueren Datums. Eine Reihe von führenden Anbietern für Hard- und Software – Microsoft®, Cisco, INTEL, Compaq und BMC – schlossen sich 1996 zu einer Initiative zusammen, um auf der Basis von Standards eine einheitliche Schnittstelle zu schaffen, die zu einer objektorientierten Behandlung der Komponenten eines IT-Systems führen soll [WBEM1]. Mitte 1998 wurde die Initiative der DMTF[6] unterstellt.

Der Vorteil dieser Initiative besteht darin, daß zwar etablierte Standards nicht angetastet, aber dahingehend erweitert werden, daß eine einheitliche Beschreibung der zu verwaltenden Umgebung geschaffen wird. Der Zugriff auf Daten erfolgt dann unabhängig vom konkreten Teil des IT-Systems stets auf demselben Weg. Dadurch werden unterschiedliche API's und Kommunikationswege vermieden, was zu einer einfacheren und gleichmäßigeren Behandlung und Korrelation aller Daten in der Unternehmens-IT als bisher führen soll. Insbesondere kann durch diese Abstraktion die vollständige Umsetzung eines objektorientierten Paradigmas, welches später noch

---

[4] Siehe Abschnitte 1.2.2 und 1.2.3
[5] Verschiedene notwendige Zusätze sind in [CMU2] definiert.
[6] DMTF = Desktop Management Task Force

genauer behandelt wird, erfolgen. Abbildung 2 zeigt den ersten Teil des Informationsschemas zu WBEM, in welchem die Objektorientierung gut zu erkennen ist.

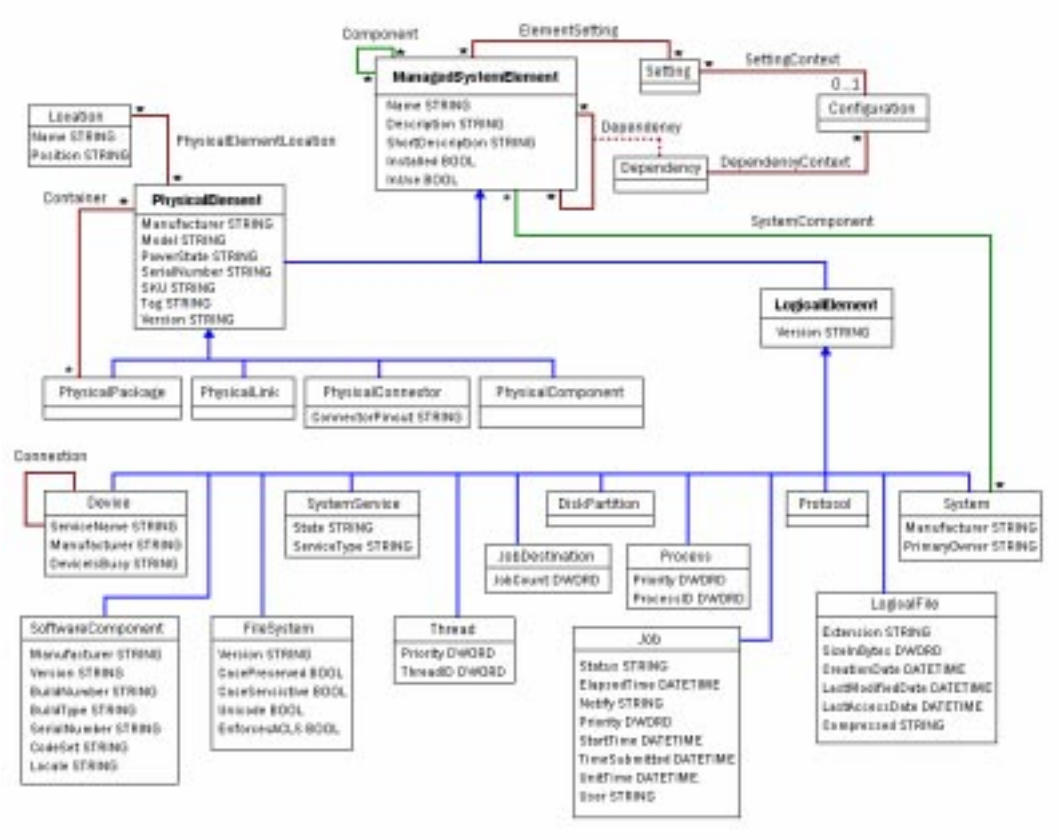

Abbildung 2: WBEM CIM-Schema v1 [WBEM3]

1.2 Klassifizierung herkömmlicher Tools

In allen Bereichen der Administration von Systemen oder Netzwerken kommen Tools zum Einsatz. Aus dem Bereich des Netzwerkmanagements kennt man die Unterteilung in drei primäre Kategorien: Diagnosetools, Monitore und Computerbasierte Managementsysteme [Held92].

Diese Werkzeuge sind unverzichtbar zur Bearbeitung fast aller Aufgaben der Administratoren. Durch verteilte Systeme mit mehreren

Standorten ist es unproduktiv, sich zu jedem Gerät physisch zu begeben, um Einstellungen durchzuführen. Oft ist die Einstellung oder der Test, insbesondere von Netzwerkkomponenten, nur durch spezielle Hardware möglich, die mitgeführt werden muß.

Die meisten IT-Systeme haben sich aus hostbasierten Systemen entwickelt. Der überwiegende Teil aller Fehler in einem solchen Umfeld wird im Netzwerk verursacht. Daher wurden große Anstrengungen unternommen, geeignete Werkzeuge zu schaffen, um diesen Fehlerquellen zu begegnen. Hersteller von Netzwerkhardware entwikkelten schon frühzeitig Programme, mittels derer ihre Hardware abgefragt und gesteuert werden konnte. Zudem ermöglichen es Agenten, die in das Netzwerk eingebracht werden, Fehler recht schnell zu erkennen. Die einzelnen Geräte werden auch immer intelligenter und lassen sich in immer höherem Umfang nur durch Software steuern und konfigurieren. Netzwerkprotokolle - sieht man einmal von Microsofts NetBEUI ab - enthalten in der Regel bereits Möglichkeiten, Fehler auf dem Übertragungsweg zu erkennen. So können in bestimmten Netzwerkkomponenten die Anzahl der verlorengegangenen Pakete, die Netzwerkauslastung und dergleichen mehr direkt abgefragt werden, ohne daß ein Softwareagent dazu nötig ist.

Werden demgegenüber Desktop-Betriebssysteme und Server-Betriebssysteme abseits von UNIX als klassischem Netzwerkbetriebssystem (bei dem Hard- und Software stets aufeinander abgestimmt sind) betrachtet, gibt es in der Systemwelt noch vergleichsweise wenig Werkzeuge. Zum einen liegt es wahrscheinlich an der höheren Komplexität der Geräte und Software, zum anderen daran, daß bisher noch keine großen Anstrengungen in Richtung Standardisierung unternommen wurden. So ist es z. B. erst seit zwei Jahren üblich, BIOS-Updates per Software direkt auf dem Motherboard durchzuführen.

Die Betriebssysteme enthalten zur Verwaltung zuwenig Eigenintelligenz. Während UNIX sich auch von einer entfernten Station administrieren läßt – durch Anmeldung via `telnet` –, muß bei anderen Systemen immer ein Zusatzprogramm gekauft werden, um administrative Aufgaben abseits der Systemkonsole zu ermöglichen.

1.2.1 Diagnosetools

Diagnosetools dienen zum Auffinden von Fehlern an Teilen des DV-Systems. Meist sind sie im Hardwarebereich eigenständige Geräte, die über Schnittstellen an Netzwerkkomponenten angeschlossen werden. Teilweise können sie aber auch in Monitore eingebettet sein. Beispiele dafür sind Mustergeneratoren und Protokollanalysatoren, aber auch Geräte zum Test von Speicherchips.

Kaum ein Betriebssystem allerdings verfügt über Diagnosewerkzeuge, da offenbar die Meinung herrscht, ein Zurücksetzen des Systems reiche aus, um Fehler zu beheben. Aus Gründen der Wirtschaftlichkeit wird dann auf eine Implementierung von Diagnosesystemen verzichtet. Viele Programme geben zwar eine Fehlermeldung aus, aber deren Dokumentation ist meistens dürftig und die Meldung selbst wenig aussagekräftig. Daher ist ein Softwarefehler, der sporadisch auftritt, sehr schwer zu diagnostizieren. Fast die einzige Ausnahme bilden hier Werkzeuge, die den Plattenstatus überwachen und Fehler am Dateisystem oder an der Plattenoberfläche melden. Diese sind in beinahe allen Betriebssystemen zu finden.

1.2.2 Monitore

Werkzeuge zum Monitoring ermöglichen es, den Betrieb und die Auslastung von DV-Systemen zu überwachen. Netzwerkseitig unterstützen die meisten Geräte bereits eine Abfrage über ihre Auslastung. Aber auch Protokollanalysatoren oder Programme zur Geschwindigkeitsmessung werden benutzt.

Viele Betriebssysteme verfügen über rudimentäre Ansätze zum Abfragen der Arbeitslast und Kapazitätsauslastung. Hardware im Desktop kann demgegenüber sehr viel seltener untersucht werden. Die Frage nach der aktuellen Auslastung einer in ein System eingebrachten Netzwerkkarte bleibt daher in der Regel unbeantwortet.

1.2.3 Probes

Probes sind physikalische Geräte, die in das Netzwerk eingebracht werden und dort Lastmessungen und Fehlersuche betreiben. Für viele verschiedene Anwendungen existieren Probes. Sie sind vor allem dort notwendig, wo Zustände des Netzwerkes mittels Software nicht feststellbar sind, jedoch eine ständige Überwachung erreicht werden soll, also ein Diagnosetool nicht eingesetzt werden kann.

Auch für Microcomputer werden in der letzten Zeit immer mehr Probes entwickelt. Sie werden zumeist in Form einer Steckkarte in das Gerät eingebaut und ermöglichen sehr weitreichende Diagnosen des Rechners. Hauptsächlich wurden sie bisher in Servern oder Systemen benutzt, die hochverfügbar gehalten werden sollen. Letzte Entwicklungen zeigen, daß angestrebt wird, diese Funktionalitäten direkt in die Hauptkomponenten eines Microcomputers (Mainboard, Netzteil, Lüfter, HDD, Graphikadapter usw.) einzuarbeiten [Ku13-98]. Damit würden auch Endgeräte im Unternehmensnetzwerk über Probes verfügen und so besser verwaltet werden können.

1.2.4 Computerbasierte Managementsysteme

Ein computerbasiertes Managementsystem stellt eine Kombination aus Hardware und Software dar, mit der die Verwaltung, also das Management, einer DV-Umgebung ermöglicht wird. Im herkömmlichen Sinne denkt man dabei an Netzwerkmanagementsysteme wie IBMs NetView oder SUNs Optivity. Sie enthalten Diagnosetools und Monitore und unterstützen den Administrator bei weitergehenden Aufgaben, indem sie Schwellwerte überwachen, automatische Maßnahmen generieren, Trouble Tickets erstellen und dergleichen mehr. Auch Produkte zum Enterprise-IT-Management, wie sie in der vorliegenden Arbeit behandelt werden, sind computerbasierte Managementsysteme. Allerdings sind sie gegenüber der ursprünglichen Definition, wie z. B. in [Held92], funktional stark erweitert worden.

1.3 Administration einer IT-Landschaft

Für die Einteilung der Administration in Disziplinen bieten sich zwei Wege an: der eine führt über den Lebenszyklus eines Netzwerks oder IT-Systems, der andere über die Aufgaben des Administrators [Fit92].

Der *Lebenszyklus* eines Netzwerkes oder IT-Systems bestimmt sich aus den Veränderungen des IT-Systems, welche durchgeführt werden, um das System ständig optimal an die Anforderungen des Unternehmens anzupassen. Das System wird geplant und implementiert. Im Betrieb wird es dann überwacht, und es werden Daten an nachfolgende Planungsschritte weitergeleitet. Es ergibt sich der in Abbildung 3 gezeigte kontinuierliche Prozeß, der häufig bei der Entwicklung von Soft- und Hardware zum Einsatz kommt, selten jedoch beim Betrieb von IT-Systemen.

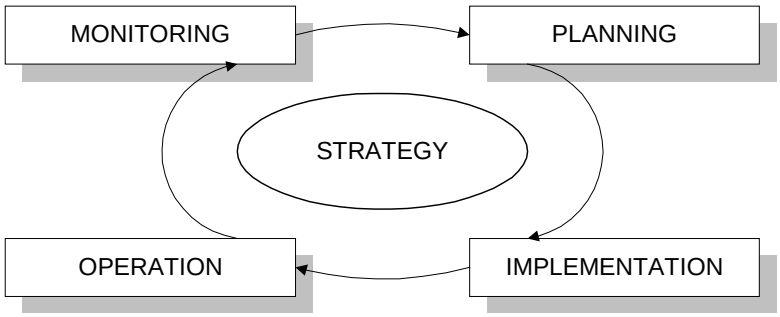

Abbildung 3: Lebenszyklus eines IT-Systems [Fit92]

Eine *funktionale Einteilung* erfolgt nach den Tätigkeiten, die Administratoren zum Betrieb des Netzwerkes ausführen müssen. Dabei handelt es sich um:

- Configuration / Change Management
  zur Erfassung und Pflege von Inventardaten über Ressourcen innerhalb der IT-Umgebung
- Fault / Problem Management
  zur Identifikation und Behebung von Fehlern
- Performance / Growth Management
  zur Messung und Änderung von Leistungsparametern
- Security / Access Management
  zur Sicherung des Netzwerks gegenüber böswilligen oder versehentlichen Angriffen und zur Authentifizierung der Benutzer
- Accounting / Cost Management
  zur Abrechnung gegenüber Kunden, aber auch zur Erfassung der durch die Bereitstellung eines Service entstehenden Kosten [ISO4].

In der vorliegenden Arbeit wurde zur Darstellung der funktionale Weg gewählt, da die Aufteilung der Abteilungen im betrachteten Unternehmen nach funktionalen Grundsätzen erfolgt ist. Die Aufzählung der Tätigkeiten, von der ISO ausgearbeitet, scheint allerdings nicht vollständig. Daher wird sie im Abschnitt 2 vervollständigt und präzisiert.

1.3.1 Trennung in Abteilungen

In jüngster Zeit wurden die Abteilungen, die für Unternehmen die IT-Umgebung warten, in hohem Maße durch Outsourcing verselbständigt. Dadurch sollte eine transparente Kostenstruktur innerhalb des Unternehmens erreicht werden. Als Nachteil dieser Entwicklung ist ein ganzheitliches Management der Unternehmenslandschaft nicht mehr möglich, da eine rechtliche Trennung des IT-Dienstleisters vom Unternehmen erfolgt.

Eine auf den ersten Blick recht einsichtige Trennung ist diejenige in Netzwerkbetreuung, System- und Clientbetreuung und Serviceabteilung für jeden einzelnen Standort, wie in Abbildung 4 illustriert. Nicht notwendigerweise wird jede einzelne Abteilung rechtlich selbständig. Die später behandelten Nachteile treten jedoch auch dann auf, wenn die Abteilungen in einem rechtlich vom Unternehmen gelösten Dienstleister zusammengefaßt werden.

Diese Struktur herrscht im betrachteten Unternehmen vor. Dabei übernimmt die Netzwerkbetreuung die Aufgaben, die dem klassischen Netzwerkmanagement zugehören, die System- und Clientbetreuung das Systemmanagement und die Serviceabteilung den Help Desk. Zentral laufen alle Störungsmeldungen des Standortes ein und werden von der Serviceabteilung an die jeweilige Fachabteilung weitergereicht. Eine davon völlig losgelöste Abteilung bearbeitet den Bereich Telekommunikation. Diese ist als eigenständiges Unternehmen aus dem Prozeß des Outsourcing hervorgegangen.[7] Jede der Abteilungen führt die Erfassung aller relevanten Daten nach den jeweiligen Anforderungen selbst durch.

Die Vorteile dieses Vorgehens liegen in einer einfachen Struktur mit klaren Zuständigkeiten. Die Einteilung kann als intuitiv plausibel bezeichnet werden.

Nachteile fallen beim Betrachten der Abbildung 4 sofort auf. Einige Aufgaben, wie z. B. Datenerfassung in ein Repository, kommen in allen Abteilungen vor. Da sie jedoch getrennt sind, werden wahrscheinlich die einzelnen Abteilungen eigene, auf ihre Bedürfnisse zugeschnittene Nischenlösungen einsetzen, die mit denen anderer Abteilungen nicht kompatibel sind. Neben einer redundanten Bearbeitung von prinzipiell gleichen Aufgaben wird damit eine erhöhte Kommunikation geschaffen, da im Falle eines komplexen Fehlers nicht eine einzelne Person Zugriff auf alle notwendigen Daten und Prozesse nehmen kann. Die notwendigen Informationen müssen vielmehr aus den einzelnen Abteilungen zusammengetragen werden. Wird das Management zudem noch unternehmensweit betrachtet, müssen an jedem Standort alle Abteilungen vorhanden sein, also liegt eine komplette Redundanz aller notwendigen Aufgabenstellungen vor.

---

[7] Der Bereich Telekommunikation wird in dieser Arbeit nicht betrachtet. Im weiteren wird der Teilbereich nur aufgeführt, um die Vollständigkeit zu wahren.

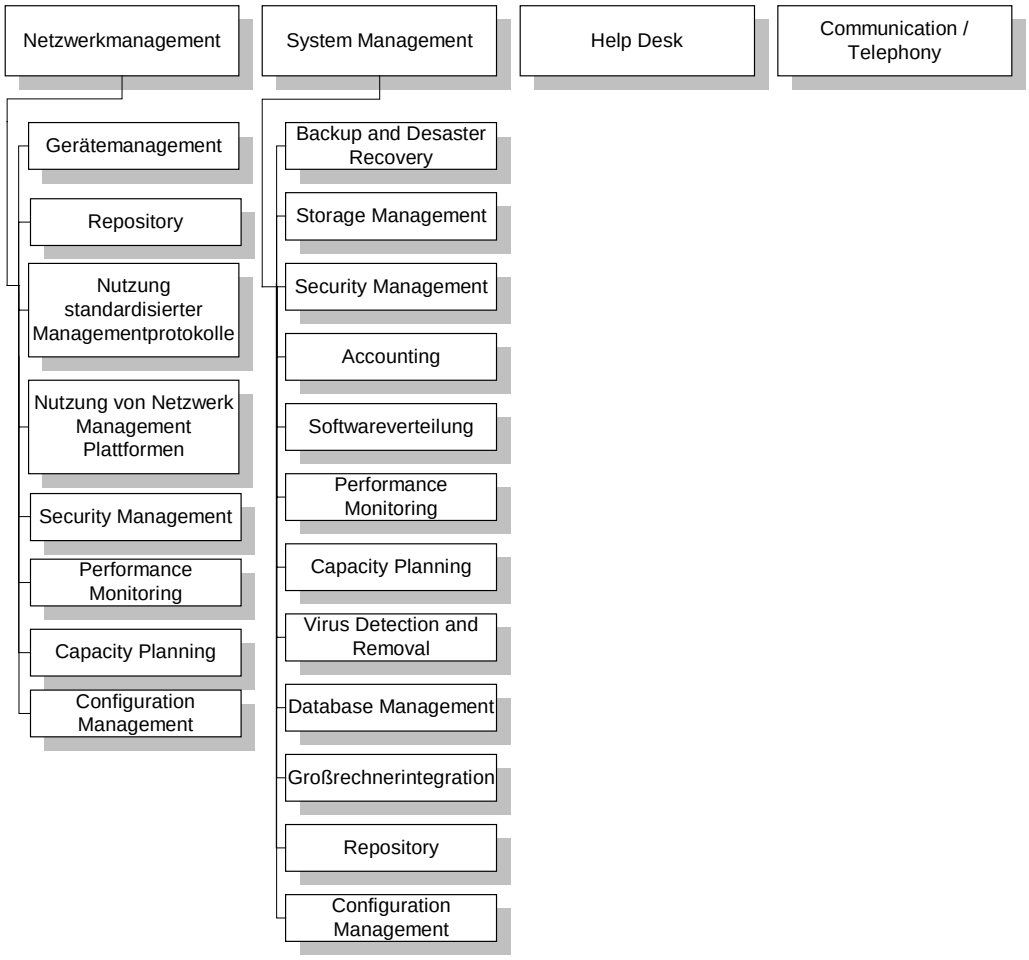

Abbildung 4: Mögliche Einteilung der Administration

1.3.2 Enterprise-IT-Management

Enterprise-IT-Management wird auch als End-to-End-Management bezeichnet. In beiden Fällen soll ausgedrückt werden, daß von einer zentralen Stelle aus alle Teile der informationstechnischen Infrastruktur eines Unternehmens voll gesteuert werden können. Eine mögliche Definition wäre:

> End-to-end management is the ability to identify specific resources throughout your IT infrastructure and then organize, monitor, and manage them. Typically, these resources are widely dispersed throughout the Enterprise. [TNG3]

Die Organisation dieses Konzeptes behandelt das gesamte Informationssystem als Einheit. Insbesondere dadurch, daß heute Telephon-, Video- und Datenverkehr über eine einzige Leitung mittels geeigneter Protokolle versandt werden, ist eine Trennung der Infrastruktur für Voicedaten von der für Computerdaten kaum noch sinnvoll. Dagegen spricht auch, daß moderne Geräte zur Telephonvermittlung Möglichkeiten der Steuerung durch Computersysteme enthalten.

Man gliedert das System nach einem objektorientierten Ansatz[8] in Klassen und Objekte, um eine effiziente Identifikation und Manipulation zu erreichen. Dadurch ist es möglich, auch abstrakte Teile des IT-Systems wie Prozesse oder „nicht-datenverarbeitende“ Bereiche wie Telephony zu integrieren (siehe Abschnitt 3.1.2).

Integration herkömmlicher Teilbereiche, *Funktionen der System Management Console*, *Ereignismanagement* und *Offenheit gegenüber anderen Managementsystemen* sind die primären Teile eines solchen Systems. Die Funktionen werden in Abbildung 5 gezeigt und im weiteren Verlauf der vorliegenden Arbeit näher untersucht.

Die Bereiche Netzwerkmanagement, System Management, Help Desk, Asset Management und Communication / Telephony werden isoliert auch in der heutigen Praxis angewandt. Sie gliedern sich wiederum in einzelne Disziplinen. Abbildung 6 zeigt diese in ungeordneter Folge, da nicht entscheidbar ist, welcher Tätigkeit die größte Bedeutung zukommt. Wichtig bei der Betrachtung von Abbildung 5 und Abbildung 6 ist, daß hier nicht mehr eine Trennung in Abteilungen erfolgt, sondern daß alle Aufgaben objektbezogen von einer Person erfüllt werden sollen. Zur Motivation dieser Vorgehensweise wird im Abschnitt 3.1 Stellung genommen.

---

[8] Das Konzept der Objektorientierung, wie in [TNG3] oder [Rum91] behandelt, wird als bekannt vorausgesetzt und nicht näher erläutert.

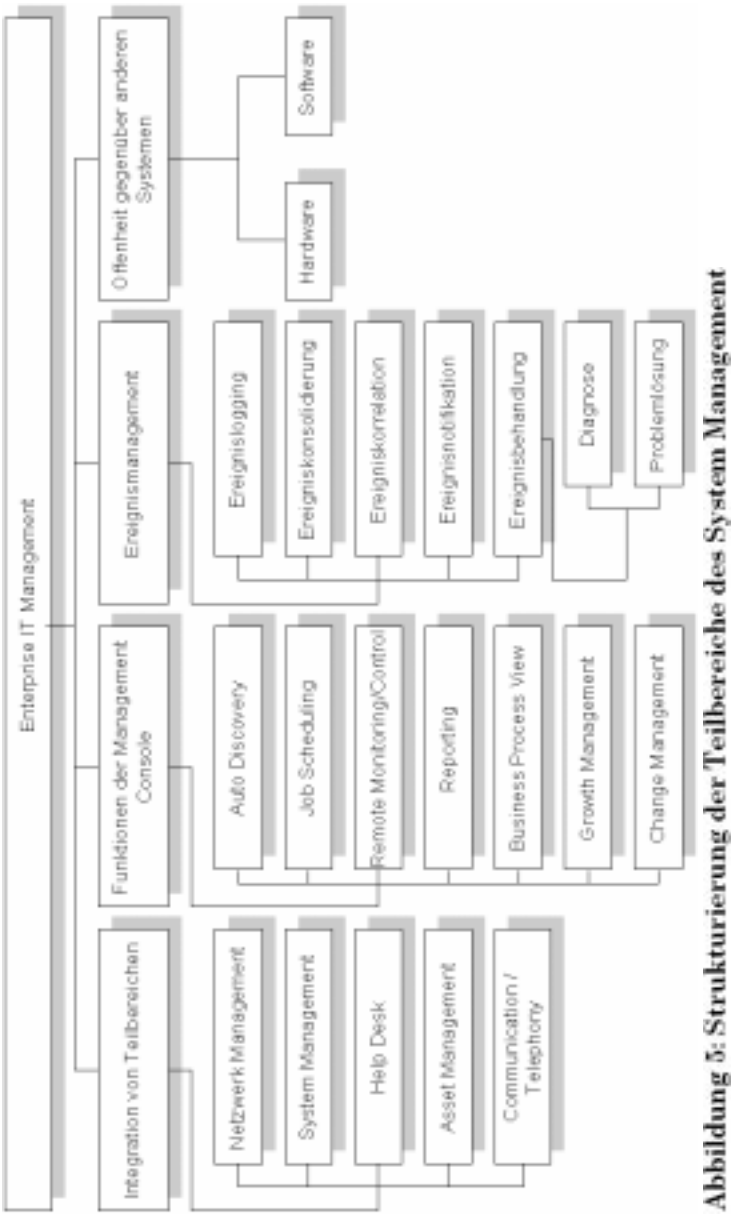

Abbildung 5: Strukturierung der Teilbereiche des System Management

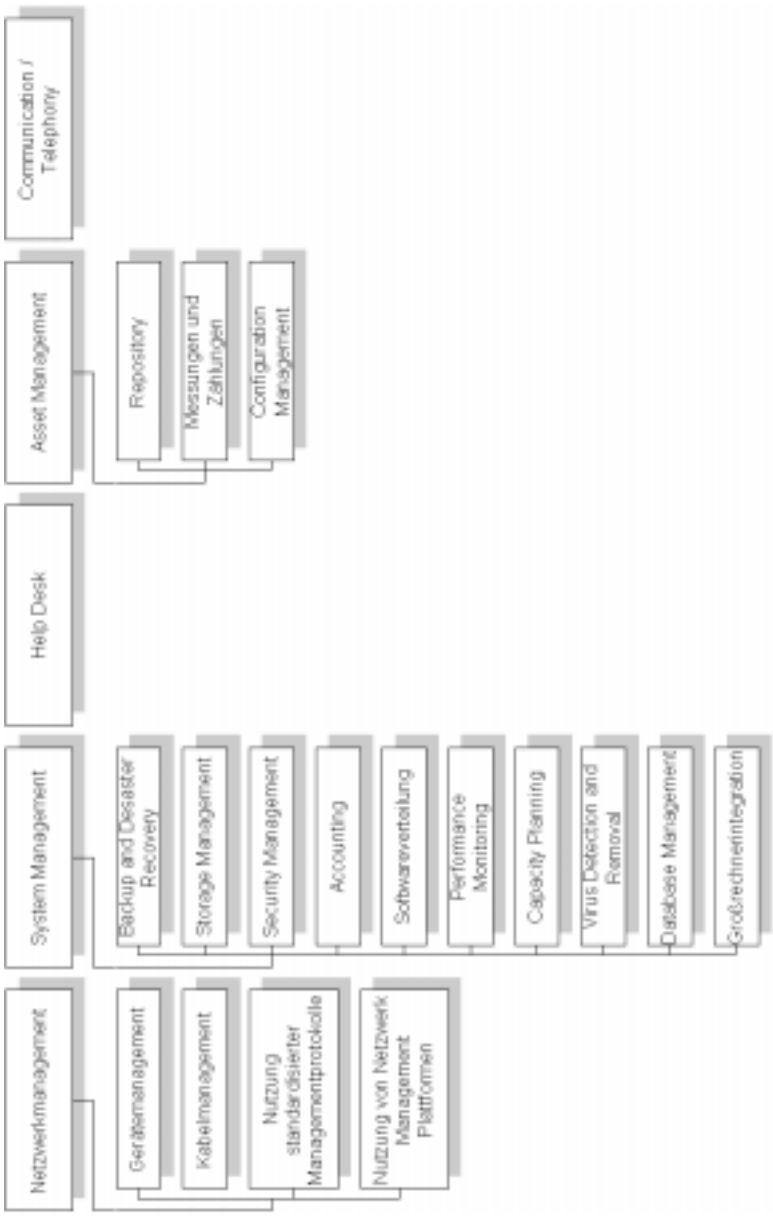

Abbildung 6: Disziplinen der herkömmlichen Administration

2 Die heutige Praxis

Die Betrachtungen der heutigen Praxis werden entsprechend Abbildung 5 und Abbildung 6 gegliedert. Leider gibt es eine geradezu babylonische Begriffsverwirrung. Begriffe werden verschieden interpretiert oder gleiche Problemstellungen mit verschiedenen Namen versehen. Hauptsächlich kommt diese Verwirrung durch Anbieter von Managementsystemen zustande, die damit Vergleiche erschweren und eine Vollständigkeit ihres Produktes suggerieren wollen.

Im folgenden Abschnitt werden die zum Enterprise-IT-Management gehörenden Begriffe präzisiert. Dabei wird sowohl auf allgemeine Literatur als auch auf Veröffentlichungen von Produktanbietern zurückgegriffen. Im allgemeinen soll die angegebene Erläuterung als Resultat des Abgleichs und Zusammenführens der unterschiedlichen Beschreibungen in der Literatur angesehen werden. Manchmal unterschieden sich die gefundenen Definitionen aber derartig, daß eine Entscheidung getroffen werden mußte. Darauf ist im jeweiligen Absatz hingewiesen. Zusätzlich werden die Beschreibungen der Begriffe mit den Ergebnissen der Untersuchung im Unternehmen Siemens Business Services GmbH & Co. OHG unterlegt.

2.1 Integration von Teilbereichen

Für alle Tätigkeiten in der Administration eines IT-Systems gibt es Tools, die für eine höhere Effizienz sorgen sollen. Die Integration dieser Tools in ein gemeinsames Konzept ist Voraussetzung für die Nutzung von Synergieeffekten, wie z. B. der Vermeidung von redundanten Tätigkeiten.

2.1.1 Netzwerkmanagement

Mit dem Netzwerkmanagement werden alle Hardwarekomponenten behandelt, die zum Austausch oder der Verarbeitung von Daten im System dienen. Dies sind alle *Geräte*, die in das IT-System eingebracht wurden, und alle Verbindungen der Geräte untereinander.

2.1.1.1 Gerätemanagement

Im IT-System befindet sich eine große Anzahl Geräte wie Server, HUBs, Switches, aber auch Arbeitsplatzrechner. Das Gerätemanagement soll alle diese Geräte konfigurieren und abfragen können und so verwaltbar machen.

Wie im ersten Abschnitt bereits erwähnt, wurde der Verwaltung des Netzwerkes bisher große Bedeutung beigemessen. So auch bei dem betrachteten Unternehmen SBS. Die Werkzeuge sind entsprechend ausgereift. An allen Standorten werden dieselben Werkzeuge für das Netzwerkmanagement eingesetzt. Es ist umfangreiches Know-how aufgebaut worden. Graphische Modellierung unterstützt die Navigation im Netzwerk. Die Geräte können remote bis auf Portebene administriert werden. Allerdings existiert kein Zugriff über Standorte hinweg, da die Zuständigkeit an Standort- bzw. Regionalgrenzen gebunden ist.

2.1.1.2 Kabelmanagement

Die Datenströme im IT-System laufen in aller Regel über Kabel. Im LAN-Bereich sind diese noch klar als physikalische Entität sichtbar. Im WAN-Bereich erfolgt die Kommunikation zumeist über Dienstleister, die eine Bandbreite zur Verfügung stellen. Diese Verbindungen sind nicht notwendigerweise an ein Kabel gebunden. Der Nutzer dieser Verbindungen verwaltet diese nicht als physikalisch, sondern als logisch. Das Kabelmanagement soll eine Transparenz für den Administrator erreichen. Störungen sollen erkannt und Parameter der Verbindungen abgefragt werden können. Weiter ist Kabelmanagement wichtig für das Design des IT-Systems, da Datenströme derartig gesteuert werden können, daß die Übertragungskosten, und zwar sowohl monetärer als auch zeitlicher Art, minimiert werden.

Aufgrund des hohen Aufwandes und weil die Verlegung der Kabel nicht durch den IT-Dienstleister SBS selbst durchgeführt wird, wird Kabelmanagement nicht durchgeführt. Auch ist eine derartige Verwaltung durch den Kabelverleger nur rudimentär vorhanden, was

aufgrund der reinen Verlegung ohne Optimierungsauftrag nicht verwundert.

2.1.1.3 Nutzung standardisierter Managementprotokolle

Zur Abfrage und Manipulation von Geräten dienen spezielle Protokolle, die im Abschnitt 1.1 näher erläutert wurden. Um eine effiziente Verwaltung der Netzwerkgeräte zu ermöglichen, soll ein weitgehend einheitliches und durchgängiges Frontend zur Manipulation von Netzwerkobjekten zur Verfügung stehen, dessen Look-and-Feel bei der Behandlung selbst unterschiedlicher Objekte gleich bleibt.

Derzeit werden bei SBS lediglich SNMP und RMON in größerem Umfang benutzt, da diese von den eingesetzten Managementplattformen gefordert werden. CMIP und WBEM wurden bisher, wenn überhaupt, nur in geringem Umfang und zu Demonstrationszwecken implementiert.

2.1.1.4 Nutzung von Netzwerk-Management-Plattformen

Für die Verwaltung von Netzwerken werden seit geraumer Zeit computerbasierte Managementsysteme eingesetzt. Diese werden meist vom Hersteller von Netzwerkgeräten geliefert und können daher alle (auch proprietären) Möglichkeiten der Geräte nutzen. Sie unterstützen bereits eine große Breite an Managementaufgaben vom Monitoring bis zur Ereignisbehandlung. Es gab und gibt Versuche, durch modulare Systeme eine einheitliche Basis zu schaffen, mittels derer Geräte verschiedener Hersteller über ein Programm verwaltet werden können. Leider sind diese Versuche als gescheitert anzusehen. Bestenfalls können alle Geräte in einem Managementsystem repräsentiert werden, bei der Konfiguration wird dann auf das jeweils vom Hersteller gelieferte Managementsystem zurückgegriffen. Zwar kann man die Informationen der MIBs einzelner Geräte auch über Managementsysteme von Fremdanbietern verändern, aber dies ist sehr aufwendig und auch nicht üblich.

Bei SBS werden im wesentlichen Netzwerkkomponenten von zwei Herstellern eingesetzt. Folgerichtig existieren zwei Managementsysteme, die parallel eingesetzt werden. Diese beiden Systeme verfügen nicht über eine gemeinsame Datenbasis. Proaktives Monitoring wäre mit den vorhandenen Werkzeugen möglich, wird aber nicht generell eingesetzt.

2.1.2 System Management

Das System Management ist begrifflich schwer zu fassen. Der Begriff wird sowohl zur Bezeichnung eines Managementsystems [Held92] als auch einer Disziplin eines Managementkonzeptes [TV1] verwandt. In Abbildung 5 ist das System Management als Teilbereich des Enterprise-IT-Management eingegliedert. Nicht zuletzt durch die herkömmliche Strukturierung von Administratoren in Netzwerk- und Systembetreuer erscheint diese Gliederung intuitiv. Im wesentlichen werden im System Management die Tätigkeiten zur Betreuung der Softwarekomponenten eines IT-Systems zusammengefaßt. Unter Software werden nicht nur Programme verstanden, sondern auch Nutzerdaten, Datenbanken und Prozesse, die zu einem Zeitpunkt im IT-System laufen.

SBS als Dienstleister für den SIEMENS-Konzern hat die Schwierigkeit, zwei grundsätzlich verschiedene Systemumfelder zu betreuen. Aus der Entwicklung des Konzerns heraus ergibt sich folgendes Bild: Während beim Kunden SIEMENS die Migration der Serverdienste auf WindowsNT fast abgeschlossen ist und nur noch spezielle Aufgaben von Unix-Rechnern erledigt werden (z. B. Netzwerkmanagement auf SUN OS), sind alle Services beim Kunden SNI auf UNIX implementiert und lediglich die Authentifizierung erfolgt an PDCs[9] und BDCs[10] auf WindowsNT.

Vor der Zusammenführung der Administrationsgruppen in einer Abteilung waren unterschiedliche Gruppen für die Kunden SIEMENS

[9] PDC – primary domain controller
[10] BDC – backup domain controller

und SNI zuständig. Dementsprechend unterscheiden sich die Werkzeuge und Verfahren zum Systemmanagement sehr stark. Zudem wird eine Integration der Verwaltung erschwert, da die Betriebssysteme über unterschiedlich stark ausgeprägte Fähigkeiten in Netzwerken verfügen und daher die einzelnen Gruppen völlig unterschiedliche Anforderungen an Werkzeuge hatten. Das führt zu einem Bruch in den Werkzeugen zum Systemmanagement, wie in den folgenden Abschnitten zu sehen sein wird. Die Homogenisierung der Werkzeuge wird zwar stark vorangetrieben, aber eine vollständige Zusammenführung wird nicht möglich sein. Auch wenn es nicht die aktuelle Organisation des Dienstleisters widerspiegelt, wird im folgenden zwischen Betreuern von SIEMENS und SNI unterschieden, um die verwendeten Werkzeuge und Verfahren unterscheiden zu können.

2.1.2.1 Backup and Disaster Recovery

Ohne Zugriff auf die als Daten gespeicherten Informationen kann heute kein Unternehmen überleben. Kaum ein Unternehmen leistet sich das Risiko, seine Daten lediglich auf den Datenträgern im laufenden Betrieb zu halten. Deren Sicherung kommt deshalb große Bedeutung zu, und sie ist Aufgabe des Backups und des Disaster Recovery. Zu sichern sind dabei nicht nur Informationen, die im Laufe der Zeit von den Mitarbeitern des Unternehmens erstellt wurden. Auch Einstellungen in Systemen, die nur mit einem hohen Aufwand an Spezialistenzeit und den entsprechenden Kosten verbunden sind, zählen zu den sichernswerten Daten.

Grundlegende Sicherungsmaßnahmen werden durch spezielle Hardware ermöglicht. Sog. RAID-Systeme[11] stellen die Daten nach Ausfall einer Platte durch redundante Speicherung der Informationen wieder her. Spiegelserver können bei Ausfall eines Servers dessen Aufgaben übernehmen. Teile eines Servers können während des Betriebs ausgetauscht werden (Hot-Swap), wie z. B. bei Netzteilen üblich. Trotz

[11] RAID ≡ redundant array of inexpensive disks (im Marketing-Schrifttum auch redundant array of independent disks)

dieser Maßnahmen können Datenverluste auftreten, so daß eine Wiederherstellung notwendig wird.

Backup und Disaster Recovery sind Begriffe, die von einigen Herstellern benutzt werden, um die Funktionsübernahme ausgefallener durch gleichartige, redundant im System vorgehaltene Komponenten zu beschreiben. Die hier verwendete – und ältere – Definition bezieht sich auf die reine Datensicherung gegen Verlust.

Backup-Systeme sichern Daten zu einem Zeitpunkt auf einen sicheren Datenträger, indem Duplikate der Originaldateien erstellt werden [Hus91]. Bänder werden als bestgeeignete Medien angesehen [Durr91]. Bei Datenverlusten durch Hardwarefehler, Benutzerfehler, Angriffe durch Viren oder Personen oder andere Typen von Fehlern kann der Zustand des Systems zum Zeitpunkt der Sicherung wiederhergestellt werden. Das Erstellen von Backups kann zentralisiert werden. Dann sichert ein Rechner alle relevanten Daten. Meist werden hierfür Bandwechsler benutzt. Der Vorteil liegt in einer vereinfachten Administration.

Disaster Recovery wird von speziellen Werkzeugen durchgeführt. Der Vorteil gegenüber Backup-Verfahren liegt darin, daß ein komplettes System praktisch ohne Vorarbeiten auch von Laien wiederhergestellt werden kann. Während zum Wiederherstellen von Daten von einem Backup zunächst die Platten partitioniert, das Betriebssystem installiert und das Backup-Programm aufgespielt und konfiguriert werden müssen, sind diese Tätigkeiten bei Disaster Recovery Produkten nicht notwendig. Gerade bei verteilten Systemen, in denen nicht jeder Standort über einen Administrator verfügt, können Mitarbeiter vor Ort Systeme wieder zum Laufen bringen, ohne daß extra ein Spezialist anreisen muß.

Bei den Betreuern von SIEMENS und SNI werden Sicherungswerkzeuge eingesetzt, die über das Netzwerk auf spezielle Backupserver im Standort sichern. Obwohl der Ansatz gleich ist, werden unterschiedliche Produkte verwendet, um damit den Eigenheiten der zugrundeliegenden Betriebssysteme Rechnung zu tragen. Die Entwicklung geht allerdings in die Richtung eines einheitlichen

Sicherungssystems. Damit werden Schwächen ausgeräumt, die durch das Einbringen anderer Betriebssysteme entstanden sind. Beispielsweise dürfte dann auch eine Sicherung der Authentifizierungsserver im SNI-Bereich erfolgen. Die Sicherung erstreckt sich nur über die Server. Clientsicherung wird standardmäßig nicht durchgeführt. Ein Benutzer kann zwar eine Sicherung anfordern, in die regelmäßige Datensicherung werden Clients jedoch nicht eingebunden.

Disaster Recovery wird nicht betrieben. Bei UNIX sind keine entsprechenden Werkzeuge erhältlich (meist sind Sicherungen nur offline möglich, was hinsichtlich der Verfügbarkeit der Server inakzeptabel ist). Im WindowsNT-Umfeld gibt es entsprechende Werkzeuge, diese kommen jedoch nicht zum Einsatz. Es ist auch nicht zu erwarten, daß Aktivitäten in Richtung Disaster Recovery aufgenommen werden, solange nicht geeignete Werkzeuge für die Unix-Systeme zur Verfügung stehen, da sonst die angestrebte Einheitlichkeit in den Backup-Verfahren wieder durchbrochen würde.

2.1.2.2 Security Management

Die hohe Abhängigkeit der Unternehmen von ihren Daten erfordert nicht nur Schutz vor Verlust, sondern auch vor unbefugtem Zugriff. Diese Aufgabe obliegt dem Security Management. Verschiedenes muß getan werden, sollen nur autorisierte Zugriffe auf das IT-System zugelassen werden.

Im OSI-Standard ist Security Management in drei Kategorien eingeteilt [ISO4]:

1. System Security Management
2. Security Service Management
3. Security Mechanism Management

Zunächst ist ein unternehmensweites Sicherheitskonzept notwendig (System Security Management), in welchem festgelegt ist, welche Sicherheitskriterien im System anzuwenden sind (Security Policy Management), wie Verletzungen festgestellt werden können (Security Audit Management) und wie ggf. darauf zu reagieren ist (Event

Handling Management, Security Recovery Management). Dann wird einzelnen Teilen des IT-Systems ein auf diesen Sicherheitskriterien basierendes Sicherheitsziel zugeordnet (Security Service Management). Zuletzt werden Mechanismen definiert, die zur Erreichung dieser Sicherheitsziele verwendet werden (Security Mechanism Management). Dazu zählen Verschlüsselung, Signaturen, Zugriffskontrolle, Datenintegrität, Authentifizierung und andere sicherheitsrelevante Punkte.

Dieses Konzept sollte im Unternehmen durchgängig sein, damit nicht, z. B. durch Umzug von Mitarbeitern, Lücken im Sicherheitssystem entstehen. In diesem Konzept sind auch Richtlinien zur Vergabe von Kennwörtern und die Kategorisierung der Sicherheitsstufen von Daten enthalten. Daten werden durch eine Risikoanalyse in diese Kategorien eingestellt [Durr91].

Dann ist eine einheitliche Implementierung notwendig. Zur Authentifikation ist eine zentrale Stelle zu empfehlen, da durch zusätzliche lokale Zugriffsberechtigungen das System leicht unübersichtlich wird. Es kann zu fehlerhaften Berechtigungen kommen. Ein hierarchisches Rechtesystem, welches im Unternehmen durchgängig angewandt wird, ist gegenüber schleichenden Fehlern recht widerstandsfähig und wird daher von Firmen eingesetzt [Kor97].

Angenommen, in einer Firma existieren zwei Standorte *A* und *B* mit je vier Servern *A1* bis *A4* und *B1* bis *B4*. Ein hierarchisches Rechtesystem könnte dann wie in Abbildung 7 dargestellt aussehen.

Dieses Modell ist sehr einfach gehalten, um das Prinzip zu verdeutlichen. Es unterstellt z. B., daß alle Benutzer Berechtigungen nur auf einem Server benötigen. Je umfangreicher die Umgebung und je verteilter die Berechtigungen werden, desto feiner kann man die Hierarchie granulieren. Es wäre denkbar, Administratoren für einzelne Prozesse, wie Datenbanken oder Benutzerverwaltung, zu bestimmen, welche keinen Zugriff auf andere Gebiete, wie z. B. die Verwaltung von Plattenspeichern, haben.

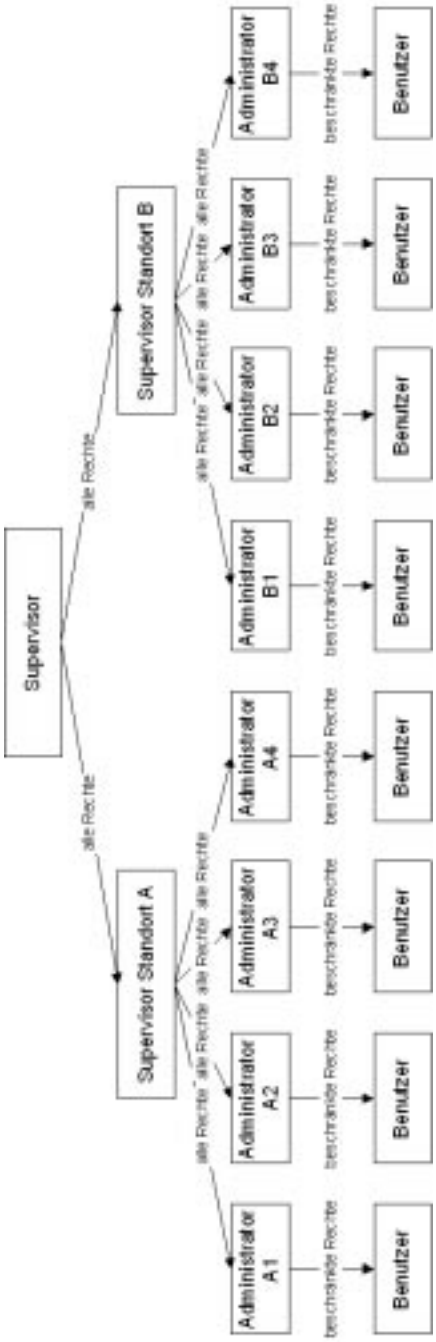

Abbildung 7: Schematische Darstellung eines Modells hierarchischer Zugriffsrechte

Die Fehleranfälligkeit eines solchen Systems ist weitaus geringer als die verteilter Strukturen. Im vorliegenden Fall sind drei Kontrollinstanzen vorhanden. Fehler (oder bewußt erstellte unzulässige Einstellungen), die durch Administratoren gemacht werden, können von den darüberliegenden Supervisorebenen erkannt und korrigiert werden und umgekehrt. Das A und O bei einem solchen Vorgehen ist die genaue Dokumentation der Änderungen (siehe Kapitel 2.2.7).

Die letzte Tätigkeit besteht in einer Kontrolle der Systemsicherheit durch nichtautorisierte Eindringversuche und dem Einsatz von Überwachungswerkzeugen.

Von einer zentralen Stelle des Konzerns SIEMENS werden Sicherheitsrichtlinien propagiert, die lokal umzusetzen sind. Diese enthalten Vorgehensweisen, nach denen das Sicherheitsmanagement ausgerichtet werden soll. An jedem Standort werden diese von der jeweiligen Systembetreuung umgesetzt. Zur Kontrolle gibt es Stichproben in Form von Eindringversuchen in die Server.

Trotz der zentralen Vorgabe der Richtlinien kommt es zu großen Unterschieden in der Umsetzung am Standort. Da die Richtlinien allgemein gehalten sind, ist jeder Administrator an seinem Standort in der Lage, eine ihm angemessen erscheinende Umsetzung vorzunehmen. So werden z. B. am Standort Düsseldorf Angriffe über nicht zum IT-System gehörende Geräte abgewehrt, indem jeder Port der Sternkoppler mit der zum dort angeschlossenen Gerät gehörigen MAC-Adresse freigeschaltet wird. An anderen Standorten wird argumentiert, daß durch das Vorhandensein abgeschlossener Gebäude eine hinreichende Sicherung besteht. Diese beiden Vorgehensweisen stellen die individuelle Umsetzung ein und derselben Sicherheitsrichtlinien dar, bieten aber stark unterschiedliche Sicherheitsstufen. Die Authentifizierung, Benutzerverwaltung und Systemverwaltung erfolgen nicht zentral, so daß diese unterschiedlichen Sicherheitsstufen nicht auffallen können.

Die Benutzerverwaltung erfolgt im wesentlichen über die Benutzerdatenbanken von WindowsNT. Teilweise haben sich die Administratoren lokale Werkzeuge geschaffen, die nur an einzelnen

Standorten zum Einsatz kommen (so in Düsseldorf eine Access-DB). Eine Verwaltung der Nutzerrechte erfolgt „bei Bedarf“, so daß von einem planmäßigen unternehmensweiten Vorgehen nicht gesprochen werden kann.

Die Kontrolle der Authentisierungsprozesse und anderer sicherheitsrelevanter Ereignisse erfolgt manuell durch das Lesen der Ereignisprotokolle des Betriebssystems. Im SNI-Umfeld kommt zusätzlich ein Überwachungswerkzeug unter UNIX zum Einsatz, das Einbruchsversuche in diese Systeme aufspüren und melden soll.

2.1.2.3 Virus Detection and Removal

Eine Gefährdung der Daten eines Unternehmens kann auch aus Computerprogrammen resultieren, deren Zweck die Schädigung von fremden Computersystemen ist. Obgleich es mehrere Typen von solchen Computerprogrammen gibt, diente der am weitesten entwickelte Typus als Namensgeber für die Tätigkeit der Abwehr durch sie verursachter Schäden – Virus Detection and Removal.

Man unterscheidet drei Arten von Schädlingsprogrammen. Sog. Trojanische Pferde sind Programme, die neben ihrer eigentlichen Funktion zusätzlich Code enthalten, der unerlaubte Aktionen ausführt. Entweder merkt der Benutzer des Programms nichts von der im Hintergrund laufenden Schadensroutine, weil das Programm fehlerfrei zu arbeiten scheint, oder das Programm selbst stellt die Schadensroutine dar. Letztgenannte Programme erwecken durch ihren Namen oder die Beschreibung Erwartungen an die Funktionalität, bei Aufruf kommt statt dessen die Schadensroutine zur Ausführung.[12] Weiterentwickelte Programme sind in der Lage, sich fortzupflanzen. Während Würmer Programme sind, deren einziger Zweck es ist, Kopien von sich selbst auf allen erreichbaren Datenträgern zu erstellen, besitzen Viren

[12] Durch die Downloadmöglichkeit von Software im Internet ist die Verbreitung von Trojanischen Pferden stark erleichtert worden. 1996 wurde ein solches Programm als neue Version des bekannten Antivirenprogramms VirusScan der Firma McAfee ausgegeben.

weitergehende Schadensroutinen. Viren sind die am weitesten entwikkelten Schädlinge, da sie nicht an eigene Dateien gebunden sind [Durr91].

Beim Virus Detection and Removal sind die folgenden Tätigkeiten notwendig:

1. Schutz des Computersystems gegen Eindringen von Schädlingsprogrammen
2. Erkennen von eingedrungenen Schädlingsprogrammen
3. Entfernen von eingedrungenen Schädlingsprogrammen

Für die letzten beiden Aufgaben stehen Werkzeuge verschiedener Anbieter zur Verfügung. Die erste Aufgabe erfordert das Erstellen eines Konzeptes, das Schwachstellen und Verbreitungsstrategien von Viren einbezieht.

Auch hier sind bei SBS die Unterschiede in der Verwaltung des Unix-Umfeldes und des NT-Umfeldes gewaltig. Da in UNIX, wenn überhaupt, nur Würmer eine schädigende Wirkung entfalten können, wurde die Abwehr auf nicht autorisierte Zugriffe beschränkt. Eine konkrete Suche nach Viren entfällt hier. Im WindowsNT-Umfeld werden Maßnahmen zum automatischen Erkennen von eingedrungenen Schädlingen vorgenommen. Das heißt, auf den Servern arbeitet Anti-Virus-Software. Diese Software leistet aber nur die unter Punkt 2 und 3 genannten Tätigkeiten. Ein Konzept zur Vermeidung des Befalls durch Einschränken der Benutzerrechte oder ähnliche Maßnahmen wird nicht betrieben.

2.1.2.4 Storage Management

Das Ziel des Storage Management ist, eine Organisation der Daten im Netz derart zu erreichen, daß einerseits die Verfügbarkeit gesichert ist und Sicherheits- und Datensicherungsstrategien gut umzusetzen sind, andererseits die Kosten der Datenvorhaltung gering sind und die Zugriffszeiten in einem angemessenen Rahmen bleiben.

Dazu eignen sich besonders gut hierarchische Konzepte, bei denen Daten von Online-Datenträgern (z. B. Festplatten) auf Nearline- oder

Offline-Datenträger (z. B. optische Jukeboxen und Bandwechsler) ausgelagert werden. Die Dateinamen (resp. deren Header) bleiben online vorhanden, so daß der Benutzer davon nicht eingeschränkt wird. Bei Zugriff auf eine ausgelagerte Datei wird diese wieder eingelagert.

Die mögliche Kostenreduktion ist enorm. Etwa 80% der Anforderungen an das Dateisystem gelten nur 20% der darauf befindlichen Daten. Weiter wird auf erstellte Dateien im allgemeinen etwa nach 30 Tagen nach ihrer Erstellung nicht mehr zugegriffen [HSM1]. Sie belegen dann nur noch Platz auf Online-Datenträgern. Werden sie nicht ausgelagert, sind Probleme wie erschöpfte Datenträgerkapazitäten oder überschrittene Plattenquoten die Folge.

Bei SBS ist das Problem als solches durchaus bekannt. Hauptsächlich wird versucht, ihm durch Quotierung entgegenzuwirken. Dies ist aber noch nicht durchgängig implementiert. Grund dafür sind vertragliche Bindungen, die aus der Zeit der Ausgründung der SBS stammen und Leistungen mit pauschalen Abrechnungsmodi vorsehen. Diese Verträge können nicht oder nur selten umgewandelt werden.

2.1.2.5 Accounting

Das Ziel der Abspaltung von IT-Abteilungen in rechtlich selbständige Unternehmen ist, eine bessere Kostentransparenz zu erreichen. Einerseits sind Abrechnungsmodi mit den anderen Unternehmensteilen zu finden, die ganz klar ausweisen, wie hoch der Anteil der IT an den Unternehmenskosten ist und andererseits sollen Dienstleistungen auch für weitere Unternehmen angeboten werden. Dazu stellen die Dienstleister den Unternehmensteilen oder Unternehmen Leistungen in Rechnung. Unglücklicherweise finden sich in der Rechnungslegung Eigenheiten, die diesem Ziel entgegenstehen. Ein möglicher Grund ist, daß eben das Accounting nicht hinreichend modelliert wurde bzw. werden konnte.

Das Accounting stellt die Daten bereit, über die eine spezielle Abrechnung für einen Kunden erst möglich wird. Dabei müssen Ressourcen des IT-Systems den Anforderungen des Nutzers entsprechend

bereitgestellt und anschließend nach dem tatsächlichen Verbrauch in Rechnung gestellt werden. Bemessungsgrundlage könnten Datenaufkommen und Rechenzeit sein.

Auch hier hat das betrachtete Unternehmen noch wenig zu bieten. Obwohl die Anbieter der Weitverkehrsnetzwerke Volumina berechnen, wird an die Kunden pauschal weiterverrechnet. Eine Abrechnung von Einzeldaten ist aber sehr kompliziert, da aus der Vergangenheit und der Entstehung durch Outsourcing teilweise alte Serviceangebote weiterbedient werden müssen, die nicht dynamisch abrechenbar sind. Außerdem ist die Rechnungslegung noch nicht in einem endgültigen Zustand. Während in der Anfangsphase versucht wurde, eine Zerlegung in kleinste Nutzungseinheiten durchzuführen, ist das Unternehmen derzeit wieder auf dem Weg, die IT als originären Teil der Betriebsausgaben zu begreifen und über Pauschalbeiträge eine Grundversorgung sicherzustellen.

2.1.2.6 Softwareverteilung

Die Landschaft eines Unternehmens ist meist weit verteilt. Nach einer Grundinstallation, die vielleicht noch an einem zentralen Standort erfolgt, werden die Rechner an den jeweiligen Arbeitsplatz gebracht. Soll nun nach einer Entscheidung der Geschäftsführung eine neue Software unternehmensweit eingesetzt oder ein Update vorhandener Daten durchgeführt werden, ist es völlig inakzeptabel, alle Rechner wieder einzusammeln und die Installationsarbeiten durchzuführen. Der Weg, einen oder mehrere Mitarbeiter vor Ort die Software aktualisieren zu lassen, ist teuer und langsam. Installationsarbeiten von den Benutzern durchführen zu lassen ist risikoreich und unter Sicherheitsaspekten nicht zu verantworten. Also müssen Installation, Aktualisierung und Verwaltung der Software möglichst bedienerlos und automatisch erfolgen. Wünschenswert dabei ist, daß ohne Neustart der Clientrechner Software verfügbar wird. Dann wird der Benutzer den Eingriff, der im Hintergrund passiert, nicht einmal

bemerken und kann die volle Laufzeit des Rechners für seine Arbeit verwenden, Server bleiben vollständig verfügbar.

Bei den hierfür zur Verfügung stehenden Werkzeugen gliedert sich der Verteilungsprozeß in *Packen der Softwarepakete*, *Planung der Verteilung* und die *Verteilung* selbst. Die Änderungen müssen protokolliert werden. Um eine überhöhte Netzlast zu vermeiden, sind spezielle Server zur Softwareverteilung zu nutzen, die parallel und kaskadierend Software vorhalten können und Profile für bestimmte Rechner erlauben.

Im Umfeld von WindowsNT wird bei SBS ein Tool eingesetzt, welches auch die Clients bedient. Teilweise kommen auch Systemmittel (z. B. login-Scripte) zum Tragen. Die Grundinstallation wird über Server oder eigens erstellte CDs durchgeführt. Alle im Zusammenhang mit Softwareverteilung möglichen Fragen werden mit den Funktionen dieses Tools beantwortet. Dadurch sind teilweise ziemlich umständliche Verfahren notwendig (z. B. für die Frage, ob sich an der Installation etwas geändert hat). Im Unix-Umfeld wird keine Softwareverteilung durchgeführt, da nicht hinreichend viele identische Verteilungsvorgänge auftreten, die den Einsatz von Software für diesen Zweck rechtfertigen würden.

2.1.2.7 Performance Monitoring

Datenbestände und Last der einzelnen Komponenten eines IT-Systems wachsen im laufenden Betrieb recht schnell. Eine neue Version einer Software stellt in aller Regel wesentlich höhere Anforderungen an Speicherplatz und Rechenleistung der Systeme. Ein Beispiel geben die Betriebssysteme selbst. Während das System Windows95 mit ca. 60 MByte Plattenplatz auskam, benötigt die Version Windows95.b bereits ca. 120 MByte. Dies stellt eine Verdoppelung bei nur einem vergleichsweise geringen Versionssprung dar. Ähnlich verhält es sich mit Nutzerdaten.

Das Performance Monitoring soll dem Verwalter Möglichkeiten bieten, kritische Zustände zu erkennen, Flaschenhälse ausfindig zu

machen und am besten *vor* Erreichen eines Überlastungszustandes geeignete Maßnahmen zu treffen.

Grundsätzlich spielt Performance Monitoring im betrachteten Unternehmen eine sehr untergeordnete Rolle. Welche Schritte in welchem Umfang unternommen werden, hängt hauptsächlich vom Engagement und der Auslastung jedes Mitarbeiters ab. Während z. B. in Köln im Bereich Netzwerke umfangreiche Dokumentations- und Überwachungsarbeiten ausgeführt werden, wird in anderen Standorten so gut wie keine permanente Analyse durchgeführt. Unternehmensweite Vorgaben existieren nicht. Dadurch befindet sich die SBS häufig in der reaktiven Rolle.

2.1.2.8 Capacity Planning

Wenn das IT-System eines Unternehmens erweitert werden soll, um neue Aufgaben zu übernehmen oder bestehende effizienter zu erledigen, müssen Planungsaspekte beachtet werden. Gute Planung und Vorbereitung sind vonnöten, da sonst die Gesamtleistung des Systems zu sinken droht [Ku7-98]. Dafür ist das Capacity Planning zuständig.

Um eine Erweiterung des Systems möglichst optimal zu gestalten, müssen alle am System beteiligten Komponenten aufeinander abgestimmt werden. Ein günstiges Vorgehen wäre die Bildung eines Projektteams aus Spezialisten, welches alle Auswirkungen der geplanten Operation feststellt und ein abgestimmtes Vorgehen entwickelt. Als Grundlage sollten nicht nur derzeitige Daten des Systems herangezogen werden, sondern auch statistische Analysen und Beobachtungen der bisherigen Entwicklung des Systems.

Ähnlich wie beim Performance Monitoring stellt sich das Bild bei der SBS im Bereich Capacity Planning dar. Beim Erweitern oder Umkonfigurieren der IT-Struktur obliegt es den damit befaßten Mitarbeitern, geeignete Schritte zu unternehmen. Dabei ist es ihnen anheimgestellt, Kollegen anderer Abteilungen in den Planungsprozeß einzubeziehen. An einem Standort wurde betont, daß stets in Zusammenarbeit von Netzwerk- und Systemspezialisten ein stimmiges

Konzept erarbeitet wird, in anderen hingegen wird ein reaktiver Ansatz verfolgt, der eine Erweiterung im Problemfall favorisiert. Neben diesen Entwicklungstätigkeiten vor Ort wird zusätzlich Know-how in Kompetenzzentren aufgebaut, welche die Kapazitätsplanung begleiten. Leider sind auch diese Maßnahmen nicht unternehmensweit oder gar konzernweit koordiniert, so daß speziell bei der Entwicklung neuer Verwaltungsstrategien kaum integrale Ansätze entstehen können.

2.1.2.9 Application Management

Die Verwaltung von Software im IT-System beschränkt sich nicht auf die im Abschnitt 2.1.2.6 angesprochenen Aufgaben, sondern erfordert auch die Überwachung der Software während der Arbeit. Die Verwaltung und Überwachung von Betriebssystemen ist selbstverständlich und bedarf keiner weiteren Erläuterung. In den folgenden Abschnitten werden deshalb nur die zwei wichtigsten Applikationsformen angesprochen. Diese Anwendungen können je nach konkreter Implementation des IT-Systems durch weitere kritische Applikationen ergänzt oder sogar ersetzt werden.

Wenn keine geeigneten Agenten zur Verfügung stehen, beispielsweise weil die Software keine Überwachungsschnittstelle bietet, können die Prozesse der Applikation über das Betriebssystem zumindest auf Abarbeitung geprüft werden, um festzustellen, ob sie noch aktiv sind. Bei Feststellen einer Fehlfunktion könnte z. B. ein automatischer Neustart des Prozesses erfolgen.

2.1.2.9.1 Database Management

Datenbanken zählen zu den wichtigsten und wartungsintensivsten Teilen des IT-Systems. Die Verfügbarkeit einer Datenbank kann bereits durch relativ kleine Fehler stark eingeschränkt werden. Auch Probleme, die vordergründig in keinem Zusammenhang stehen, können einander beeinflussen. So kann ein Überlaufen von Protokolldateien dazu führen, daß keine Operationen über der Datenbank mehr möglich sind. Eine Verletzung der Konsistenz kann zur Zerstörung der

kompletten Datenbank führen. Aus diesen Gründen erhielten die Datenbanken als einzige Softwareprozesse auch in der Vergangenheit schon besondere Aufmerksamkeit. Es gibt bei Datenbanken namhafter Hersteller Verwaltungswerkzeuge mit außerordentlichem Funktionsumfang. Diese Werkzeuge arbeiten jedoch in aller Regel direkt mit einem Datenbanksystem zusammen. Daher kann man sich nur mit der jeweiligen Konsole, auf der die Datenbank läuft, verbinden und Manipulationen oder Zustandsabfragen durchführen.

In großen IT-Systemen ist eine solche Vorgehensweise sehr zeitraubend und daher teuer. In enger Verbindung mit dem Job Scheduling / Process Management sind zentrale Konsolen anzustreben, die eine Verwaltung aller Datenbanken im IT-System erlauben. Ziel dieser Entwicklung muß die vollständige Integration von Datenbankprozessen in das unternehmensweite Job Scheduling sein. Dazu bedarf es Vorarbeiten, um die Transparenz der Datenbanken zu erhöhen.

Da die integrierten Konsolen zumindest in nächster Zeit noch ein Wunsch bleiben werden, ist die Datenbankverwaltung bei SBS remote möglich, aber wie schon erwähnt nur mit den Herstellerwerkzeugen, die den Nachteil haben, nur Datenbanken dieses einen Herstellers – und manchmal auch nur eine einzige davon – verwalten zu können.

2.1.2.9.2 SAP R/3, Baan

Viele Unternehmen haben System R/3 oder Baan zur Unterstützung der Geschäftsprozesse und Steigerung der Effizienz des Unternehmens eingeführt. Entsprechend ist die Abhängigkeit von diesen Systemen gestiegen.

Grundsätzlich gilt für diese Anwendungen dasselbe wie für Datenbanken (siehe vorheriger Abschnitt). Auch hier stehen lokale Administrationswerkzeuge zur Verfügung, eine vollständige transparente Integration in eine zentrale Konsole ist anzustreben.

Im zugrundeliegenden IT-System werden allerdings keine SAP-Installationen betreut. Diese Dienste werden von zentralen Rechenzentren übernommen.

2.1.2.10 Großrechnerintegration

Trotz der stetigen und schnellen Weiterentwicklung der Minicomputer werden Großrechner auch in naher Zukunft eine Rolle in der unternehmerischen Datenverarbeitung spielen. In vielen großen IT-Umgebungen wird die Situation noch wie in Abbildung 8 am Beispiel von Computer Associates dargestellt aussehen. Einerseits liegt das an dem in den Großrechnern verwalteten Datenstamm und andererseits an der Kapazität auf speziellen Gebieten, die von Minicomputern und Microcomputern derzeit nicht erreicht wird. Großrechner werden von den Benutzern in aller Regel über Gateways angesprochen, die Terminalfunktionalitäten auf dem Arbeitsplatzrechner anbieten.

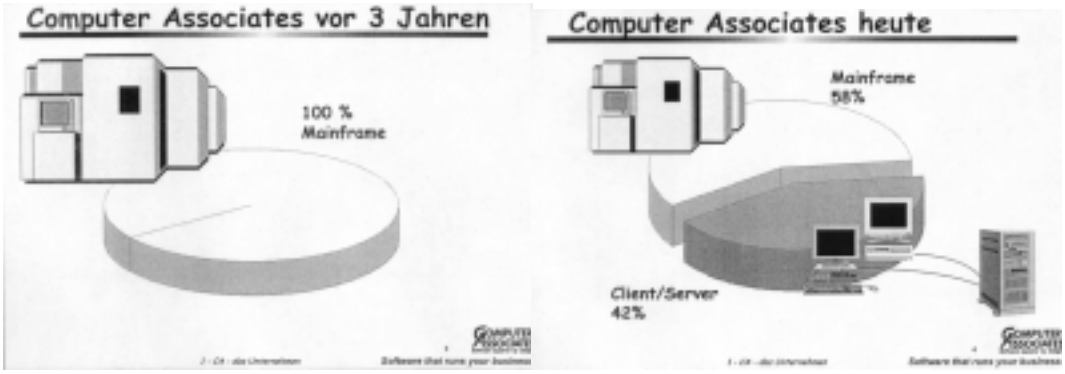

Abbildung 8: Wandel der IT-Umgebung am Beispiel Computer Associates [Leb98]

Großrechner besitzen im allgemeinen keine Standardschnittstellen. Sie kommunizieren über proprietäre Protokolle mit den angeschlossenen Clients, auch wenn es in letzter Zeit bei einigen Hostsystemen Entwicklungen in Richtung Nutzung von Standardprotokollen gibt. Es darf jedoch nicht dazu kommen, daß die Großrechner aus der Modellierung und Steuerung des IT-Systems herausfallen. Daher müssen Möglichkeiten zur Integration solcher proprietärer Systeme geschaffen werden.

Im betrachteten Unternehmen werden BS-2000-Großrechner eingesetzt. Überwiegt WindowsNT im Umfeld, laufen die entsprechenden Anbindungsemulationen auf NT-, sonst auf UNIX-Gateways. Die

Administration der Großrechner erfolgt auch hier durch zentrale Rechenzentren, so daß die Modellierung von Geschäftsprozessen, die Großrechner involvieren, zumindest erschwert ist.

2.1.3 Help Desk

Für den Kunden eines IT-Dienstleisters ist der Help Desk zentrale Annahmestelle für Störungsmeldungen und Konfigurationswünsche. Für den IT-Dienstleister selbst hat der Help Desk weitere Aufgaben. Er soll die Probleme, die von Laien angebracht werden, mit möglichst genauer Spezifizierung an die entsprechenden Fachabteilungen weiterleiten. Des weiteren sollen kleinere Probleme mit bekannten Ursachen direkt am Help Desk gelöst werden. Dazu braucht der Help Desk eine Datenbank mit Problembeschreibungen und zugehörigen Lösungen. Mit der Zeit wird der Datenbestand wachsen, und eine immer größere Zahl an Problemen kann direkt am Help Desk gelöst werden. Als Ziel kann z. B. die direkte Behandlung von 80% aller Anrufe am Help Desk angesehen werden [Brü98].

Neben dieser Datenbank wird eine Entscheidungshilfe benötigt. Als besonders gut geeignet (auch wegen einfacher Implementierungsmöglichkeit) erweisen sich (binäre) Entscheidungsbäume. Damit wird sichergestellt, daß die Mitarbeiter am Help Desk nicht auf eine falsche Spur gesetzt werden, weil z. B. durch Zeitdruck eine Möglichkeit nicht berücksichtigt wurde. Zwar werden dann auch solche Fragen an den Kunden gestellt, die dieser als unnötig ansehen könnte (Bei der Meldung „Drucker druckt nicht“ wird gefragt „Ist der Drucker eingeschaltet“), doch würde die Frage nicht gestellt, könnte ein solches „primitives“ Problem eine längere Fehlersuche nach sich ziehen.[13]

Ein zentraler Help Desk ist bei SBS CS West im Aufbau. Momentan werden alle Anfragen gesammelt und in ein Werkzeug eingegeben,

[13] In Gesprächen mit Mitarbeitern des Help Desk der Firma SBS GmbH & Co. OHG wurde festgestellt, daß diese sich scheuen, solche Fragebäume konsequent abzuarbeiten, weil einige Kunden dann – vermeintlich in ihrer Ehre gekränkt – unfreundlich werden.

welches für die Weiterleitung und Eskalation verantwortlich ist. Die Umsetzung ist aber noch nicht vollständig gelungen. Daher wird an einigen Standorten immer noch mit Papier gearbeitet, was die Priorisierungsfunktion des Help-Desk-Werkzeugs außer Funktion setzt. Das Ziel, kleinere Probleme direkt am Help Desk zu lösen, wird derzeit umgesetzt. Dazu wird hochqualifiziertes Personal in den Help Desk eingestellt. Zu den Nachteilen dieses Verfahrens wird in Abschnitt 3.2.1.3 ausführlich Stellung genommen.

2.1.4 Asset Management

Ein *Asset* ist per definitionem ein „Ding von Wert in jemandes Besitz“ [MW1]. Im hier betrachteten Kontext umfaßt dies nicht nur die Hard- und Software, die angeschafft wurde, sondern auch Personal, Arbeitsleistung, Rechenzeit usw., also alle an der Datenverarbeitung beteiligten Komponenten. In strikter Auslegung der Definition gehörten sogar Gebäude, Dienstfahrzeuge und dergleichen zu den Assets des IT-Systems. Eine gemeinsame Behandlung aller Assets eines Unternehmens ist jedoch selten sinnvoll.

Je nach Größe der Firma muß eine Fragmentierung der Assets erfolgen, damit die Datenmengen in befriedigender Weise verarbeitet werden können. Diese Fragmentierung sollte prozeßorientiert erfolgen. Dienen Dienstfahrzeuge der Problembehandlung an Außenstandorten, so gehören sie zweifelsohne zu den Assets des IT-Systems. Befördern sie jedoch lediglich den Geschäftsführer, ist die Zuordnung zu diesem Bereich zumindest strittig. Die Abgrenzungen müssen in dem jeweiligen Unternehmen nach dessen Geschäftsprozessen durchgeführt werden.

Da SNI und SIEMENS aus Unternehmen mit unterschiedlicher IT-Struktur hervorgegangen sind, verfügen sie über verschiedene Tools zum Asset Management. Die Systeme sind nicht kompatibel und zeichnen sich durch unterschiedliche Funktionalität aus. Eine Zusammenfassung wird angestrebt. Dabei wird der Funktionsumfang beider Werkzeuge in dem weiterhin einzusetzenden vereinigt.

2.1.4.1 Repository

Das Repository stellt die Informationsbasis zur Verwaltung des IT-Systems dar. Es ist nicht notwendigerweise als einzelne Datenbank implementiert. Eine Gruppe von Datenbanken mit einem Verwaltungssystem, welches alle Datenbanken steuert und Abfragen über mehrere oder alle Datenbanken gestattet, ist ebenso geeignet.[14]

Ein einheitliches Repository über alle IT-Ressourcen ist bei SBS nicht implementiert. Vielmehr gibt es für jeden Teilbereich Insellösungen, die meist nicht mit anderen Datenbeständen in Verbindung gebracht werden können. Alle Gruppen, die in Abschnitt 2.1 beschrieben sind, verfügen über eine mehr oder weniger umfassende Datenbank. Das resultiert aus der Tatsache, daß Lösungen problemorientiert gesucht und optimiert werden, eine mögliche systemorientierte Integration dabei aber nicht berücksichtigt wird.

2.1.4.2 Configuration Management

Der Begriff des Configuration Management ist aus dem Bereich des Netzwerkmanagements bekannt. Dort meint er die Verwaltung verschiedener Netzwerkgeräte. Wird „Netzwerkgeräte“ durch „Objekte im IT-System“ ersetzt, entsteht eine analoge Definition: Configuration Management ist die Verwaltung verschiedener Eigenschaften von Objekten im IT-System [Held92].

Die Tools zum Asset Management bei SBS enthalten zumindest die Datenbasis der Konfigurationen. Zwei gravierende Schwachpunkte sind beiden Systemen eigen. Erstens können keine Verbindungen zwischen Komponenten des IT-Systems modelliert werden, so daß für Leitungswege und Routinginformationen andere Datenbestände benutzt werden müssen. Zweitens bestehen keine Schnittstellen zur Manipulation der Konfigurationen. Wird eine Änderung am IT-System durchgeführt, müssen also alle Daten manuell eingepflegt werden. Bei hohen

[14] In bestimmten Fällen ist eine Gruppe von Datenbanken sogar besser geeignet, da bei hohen Datenmengen die Informationszusammenstellung nach einer Abfrage u. U. zu aufwendig sein kann.

Arbeitsbelastungen zeichnen sie sich deshalb durch wenig Aktualität aus. Rechteverwaltung, Portbelegungen und dergleichen sind in den Datenbeständen nicht enthalten und können nur in den Konfigurationsdateien selbst abgefragt werden.

2.2 Management Console

Die Management Console stellt das Interface zwischen Benutzer und Managementsystem zur Verfügung. Dazu bereitet sie die Daten zur Kommunikation mit dem Benutzer auf. Alle Einstellungen, die vorzunehmen sind, sollen weitgehend intuitiv angeboten werden, d. h. für den Benutzer muß sich weniger die Frage „*Wie* bediene ich das Werkzeug?“ als vielmehr die Frage „*Was* soll erreicht werden?“ stellen.

Eine einheitliche Management Console existiert bei SBS derzeit nicht. Die Werkzeuge enthalten je nach Aufgabe zwar bestimmte Merkmale, die eine Managementkonsole erfüllen muß, aber keines integriert sie.

2.2.1 Auto Discovery

Ein IT-System ist permanenten Veränderungen unterworfen. Ein Hauptproblem in der heutigen Unternehmenslandschaft ist, daß die Administratoren durch die Komplexität ihres Systems kaum Zeit haben, die Pflege der Dokumentation hinreichend zu verfolgen. Deshalb wird eine Möglichkeit benötigt, die automatisch auf Veränderungen des Systems aufmerksam macht und diese in die verschiedenen Datenbanken (z. B. Configuration Management, Change Management) einpflegt. Idealerweise erfüllt das Auto Discovery diese Forderung weitgehend eigenständig.

Die bei SBS verwendeten Werkzeuge zum Netzwerkmanagement enthalten Grundfunktionen des AutoDiscovery. Netzwerktopologien sind auch mittels dieser Produkte modellierbar. Im Systembereich werden Funktionen von SMS genutzt, welches eine Datenbank mit den angeschlossenen (und mit SMS-Clients ausgestatteten)

Arbeitsstationen und Servern pflegt. SMS hat jedoch die große Schwäche, nicht sehr plattformtolerant zu sein [Geb96].

2.2.2 Job Scheduling / Process Management

Rechenzeit ist im IT-System ein kostbares Gut. Nicht alle Anforderungen an das System müssen sofort bearbeitet werden. Vielmehr ist es bei einer großen Zahl an Anforderungen so, daß diese durchaus außerhalb der Hauptbelastungszeit bearbeitet werden können (z. B. Backup-Prozesse nachts). Die Antwortzeiten des Systems werden dadurch kurz gehalten, weil interaktive Prozesse möglichst effizient ablaufen können. Für das Systems Management braucht man eine Möglichkeit, systemweit Prozesse zu planen. Umgekehrt muß auch die augenblickliche Prozeßsituation abgefragt und ggf. verändert werden können. Diese Aufgaben sind im Job Scheduling / Process Management zusammengefaßt.

SBS benutzt Jobplanung nur im Zusammenhang mit den nachts automatisch ablaufenden Datensicherungen. Diese Planung wird von den Backup-Werkzeugen unterstützt. Daher sind keine separaten Werkzeuge zum Job Scheduling im Einsatz.

2.2.3 Remote Monitoring / Control

Zur Fehlersuche oder zur Konfiguration von Geräten oder Prozessen im IT-System ist es in einigen Fällen nicht möglich, mittels Werkzeugen über Schnittstellen auf ein System zuzugreifen. Insbesondere gilt das für Endgeräte, die bei Benutzern des IT-Systems laufen. Dann muß sich der Betreuer physisch zu dem Gerät begeben. Um dies zu vermeiden, muß die Möglichkeit geschaffen werden, von einem entfernten Arbeitsplatz aus die Kontrolle über ein Gerät im IT-System zu übernehmen, als säße man direkt davor. Dies soll das Remote Control leisten. Möglich wird es durch Export von Bildschirminhalten, Softwaresteuerungen von Netzwerkgeräten usw. Auch die Abfrage der aktuellen Leistungsparameter muß von entfernten Stationen aus möglich sein – durch Remote Monitoring. Die Management Console muß

beide Funktionen integrieren, damit sie direkt bei der Bearbeitung einer Komponente des IT-Systems zur Verfügung stehen.

Im Unix-Bereich enthalten die Betriebssysteme hinreichende Funktionen zum Remote Control. SBS verwendet bei NT und den Windows-Clients – abhängig von der zur Verfügung stehenden Bandbreite – zwei unterschiedliche Werkzeuge. Im LAN wird die Produktfunktion des SMS eingesetzt, welche aber hohe Anforderungen an die Bandbreite stellt, so daß bei WAN-Verbindungen ein schmalbandigeres Werkzeug zum Einsatz kommt.

2.2.4 Reporting

Unterschiedliche Personengruppen haben Interesse an verschiedenen Daten aus dem IT-System. Sei es aus Datenschutzgründen oder einfach nur, weil die betreffende Person aufgrund ihres zu geringen Sachverstandes keinen Zugriff bekommt, um Schaden vom System abzuwenden, darf sich nicht jede dieser Personen diese Daten selbst beschaffen. Trotzdem sollen die Wünsche nach Informationen aus dem System befriedigt werden. Dazu muß die Management Console in der Lage sein, Reports für die verschiedensten Gruppen von Personen zu generieren und zwar genau auf deren Bedürfnisse zugeschnitten. Idealerweise erfolgt das Reporting mittels dynamisch generierter HTML-Seiten, weil diese dann im Intranet mit einem beliebigen WWW-Browser angesehen werden können und keine zusätzliche Entwicklungsarbeit anfällt.

Bei SBS werden Reports derzeit von den Mitarbeitern auf Anforderung erstellt. Einige Mitarbeiter führen eigene Dokumentationen, die bei Bedarf sofort vorgelegt werden können, andere erstellen diese im Anforderungsfall. Automatische Reports werden generell nicht erstellt. Auch Datensammlungen über die Nutzung der Ressourcen werden nur selten erstellt.

2.2.5 Business Process Views

Business Process Views ist eine der wichtigsten Komponenten eines guten Enterprise-IT-Management. Auch wenn ein Managementkonzept in der Lage ist, sofort einen kritischen Zustand in einem Teil des IT-Systems zu melden, ist diese Information allein zu wenig, um effizient reagieren zu können. Die Folgen eines Ausfalls müssen modellierbar sein. Dazu ist es notwendig, die Management Console bei der Anzeige der IT-Struktur verändern zu können, idealerweise am Objekt selbst. Von topologischen Zusammenhängen wird abstrahiert und auf funktionale Zusammenhänge umgestellt. Es ergibt sich ein funktionaler Strang, in den das betreffende Objekt eingebunden ist. Dadurch kann man sofort ablesen, welche Probleme nach Ausfall eines speziellen Objektes zu erwarten sind.

Die umfassende Modellierung des IT-Systems nach dieser Maßgabe ist unabdingbare Voraussetzung für die Ereigniskorrelation, wie später noch erläutert wird.

Leider ist zum jetzigen Zeitpunkt eine Modellierung der Prozesse im betrachteten Unternehmen nicht üblich.

2.2.6 Growth Management

Unter „Wachstumsverwaltung“ kann man sich zunächst nur schwer etwas vorstellen. Auch wird nicht eigentlich das Wachstum verwaltet, sondern die Voraussetzungen für das Wachstum werden geprüft und Änderungen archiviert. Wichtig ist das vor Änderungen am IT-System. Da das Wachstum eines IT-Systems dieses verändert, wird das Growth Management häufig als Bestandteil des Change Management (siehe nächster Abschnitt) angesehen

Zur Illustration soll ein Beispiel dienen. In einer Firma wird die Migration von Windows 3.11 auf WindowsNT 4.0 Workstation geplant. Von den derzeit 200 Arbeitsplatzrechnern eignen sich 93 für den Umstieg, bei 47 muß der Arbeitsspeicher erweitert werden, bei 16 ist der Umstieg nicht möglich, weil Hardwarekomponenten nicht unterstützt

werden, 4 Rechner brauchen eine neue BIOS-Version und 40 Rechner sind zu alt, so daß eine Umrüstung nicht lohnt.

Wie in diesem Beispiel müssen Informationen, die vor der Änderung zur Verfügung stehen, mit den bestehenden Tatsachen verglichen werden, um z. B. eine Kostenschätzung vornehmen zu können. Voraussetzungen sind nicht nur eine gut gepflegte Datenbank über die Assets der Unternehmung, sondern auch ein Werkzeug zu Abfrage und Verarbeitung der Informationen. Natürlich ist diese Planungstätigkeit auch manuell durch schrittweises Vergleichen der Eigenschaften vorhandener Objekte mit den Anforderungen der gewünschten Änderung möglich, je mehr unterschiedliche Objekte jedoch zu behandeln sind, desto zeitaufwendiger wird das Unterfangen.

Nach Abschluß der Erweiterung müssen die Änderungen dokumentiert werden. Ziel der Dokumentation ist die Aussagefähigkeit über Kosten von Veränderungen und damit eine Kostentransparenz.

2.2.7 Change Management

Ein IT-System zu implementieren und dann unverändert einzusetzen, ist in den seltensten Fällen möglich. Durch neue Anforderungen an ein System sind ständig Änderungen und Optimierungen nötig. Werden diese nicht ausreichend dokumentiert, sind Probleme nur eine Frage der Zeit. Auch wenn am Anfang noch alles funktioniert, kann eine Änderung ein System langfristig in Schwierigkeiten bringen. Da zwischenzeitlich wohl auch andere Änderungen durchgeführt werden, ist die Suche nach dem Verursacher schwierig, wenn nicht aussichtslos. Möglich sind auch Interdependenzen zwischen Änderungen, die letztlich zum Problem führen. In extremen Fällen kann eine Neuinstallation notwendig werden. Das Change Management unterstützt die Veränderungen durch Planung und Dokumentation der durchgeführten Maßnahmen.

Da allgemein gilt, daß die Dokumentation von Änderungen, die nach Meinung des Administrators lediglich marginal sind, häufig unterlassen wird, könnte der Idealfall ein automatisch mitschreibendes

System sein. Gerade diese kleinen Änderungen sind es, die vergessen werden können und bei einer Rekonstruktion des Änderungsvorgangs aus dem Gedächtnis nicht mehr berücksichtigt werden. Legt man jetzt noch ein objektorientiertes Verwaltungssystem, wie es später entwikkelt wird, zugrunde, ist eine Dokumentation aller Änderungen unumgänglich, da nicht wie bisher eine Person an immer dem gleichen Teil des IT-Systems arbeitet. Während bei der ständigen Betreuung eines bestimmten Teiles der Administrator „mitwächst" und „sein Reich" kennt, benötigt er bei Objektmanipulationen eine genaue Dokumentation zur Entwicklung des Objektes, weil hierbei alle Abteilungs- und Standortgrenzen hinfällig werden.

Bei SBS werden weder Growth- noch Change-Daten erhoben. Die starke Lokalität und die Verwaltung durch „Brain Management" führen dazu, daß lediglich die Administratoren Kenntnisse über vorgenommene Änderungen haben. Die Nachteile kommen voll zur Geltung. Es gibt unbestreitbar auch Vorteile eines solchen Verwaltungsansatzes, wie z. B. die große Kundennähe und die Nähe zu den IT-Ressourcen. Ob dies aber die Nachteile hinsichtlich des erhöhten Arbeitsaufwandes durch fehlende Dokumentation aufwiegt, darf bezweifelt werden.

2.3 Ereignismanagement

Dem Ereignismanagement kommt auf der Seite des Managementsystems die größte Bedeutung zu. Ein laufendes System interessiert den Administrator, dessen primäre Aufgabe die Aufrechterhaltung der Verfügbarkeit des Systems ist, wenig. Bestenfalls das übergeordnete Management ist an einigen Kennzahlen aus dem System interessiert. Entsprechend des Unix-Grundsatzes *„No news are good news."* werden also nur dann Ereignisse „erzeugt"[15], wenn ein Versuch des Systems

[15] Im allgemeinen Sprachgebrauch hat es sich durchgesetzt, von Events, also Ereignissen, als Dingen zu sprechen, die im sog. Ereignisprotokoll eines Programms festgehalten werden. Diese Einträge sind aber nur die Fehler oder Informationen, die als protokollierungswürdig angesehen wurden. Daher kann man durchaus von der Erzeugung von Events durch das Programm sprechen.

oder eines Nutzers, einen Befehl auszuführen, fehlgeschlagen ist oder vom Administrator als zu protokollierend markiert wurde.

Alle Zustände des Systems sollen hier zentral verwaltet werden können. Zudem soll eine Dokumentation stattfinden, die es erlaubt, die Entwicklung des Systemzustandes zu verfolgen oder Aussagen darüber zu treffen, in welchem Zustand das System zu einem Zeitpunkt *X* war.

Alle Tätigkeiten, die im folgenden besprochen werden, sind bei der SBS mehrheitlich manuell abgedeckt. Die Konsolidierung erfolgt über Durchlesen und Sichern der Protokolldateien, die Korrelation wird vom zuständigen Administrator durchgeführt. Diese Vorgehensweise ist keinesfalls ineffektiv oder unzureichend, eignet sich aber hervorragend zur Automatisierung. Außerdem würde durch eine Automatisierung das bisher damit befaßte hochqualifizierte Personal zeitlich stark entlastet.

2.3.1 Ereigniskonsolidierung

Die erste und einfachste Aufgabe innerhalb des Ereignismanagements ist das Aufzeichnen aller Ereignisse in speziellen Dateien oder Datenbanken. Fast alle Betriebssysteme bieten die Möglichkeit, Meldungen des Systems in dedizierten Dateien abzuspeichern und später auszuwerten. Die Ereigniskonsolidierung, teilweise auch als *Ereignislogging* bezeichnet, erweitert diese Funktionalität dergestalt, daß die Speicherung der Ereignisse in dem zentralen Repository stattfindet und nicht auf der lokalen Maschine unter den manchmal doch recht kryptischen Namen an mehr oder minder versteckten Orten. Diese Zentralisierung ist für alle nachfolgenden Schritte Voraussetzung.

Erreicht werden kann dies, indem z. B. die Systemlogs laufend auf neue Einträge überprüft und diese in das Repository übernommen werden.

2.3.2 Ereigniskorrelation

Unter der Korrelation von Ereignissen wird das Finden von (möglicherweise ursächlichen) Verbindungen zwischen Ereignissen

verstanden. Diese Aufgabe hat bisher der Help Desk zu leisten. Die Komplexität dieser Aufgabe ist relativ hoch, kann jedoch teilweise automatisiert werden.

Im wesentlichen können drei Arten von Ereignissen unterschieden werden. Zunächst gibt es solche, die als elementar bezeichnet werden können. Sie hängen von keinem weiteren Ereignis ab. Beispiele dafür sind der Ausfall eines Lüfters oder einer Festplatte. Hier ist die Korrelation einfach, weil einstufig. Der zweite Typ sind Ereignisse, deren Ursache komplex, d. h. mehrstufig, ist und automatisch aufgelöst werden kann. Ein Beispiel wäre eine abgebrochene Datenbanktransaktion nach Ausfall eines Routers. Wenn ein automatisches Korrelationswerkzeug über hinreichend Intelligenz verfügt, wird es die beiden Ereignisse in der Datenbank in Beziehung setzen. Hier ist allerdings auf die Business Process Views zu verweisen, weil nur mit einer solchen, aktuellen Datenbasis „Wirkungsstränge“ modelliert werden können. Die dritte Gruppe sind Ereignisse, deren Ursachen nicht automatisch aufgelöst werden können. Hauptsächlich sind dies Ursachen, die die Intelligenz des Systems übersteigen, sowie Designfehler.

2.3.3 Ereignisnotifikation

Nachdem eine Korrelation der anfallenden Ereignisse stattgefunden hat, muß das Ereignis dem Help Desk bekannt gemacht werden. Wichtig ist, daß diese Bekanntmachung *nach* der Korrelation erfolgt. Sonst würde für den Fall, daß ein zentrales Netzwerkgerät ausfiele und ein komplettes Teilnetz nicht mehr erreichbar wäre, für jedes überwachte Objekt ein Ereignis generiert, und die Übersicht ginge verloren. Außerdem könnte das Unternehmensnetzwerk durch einen sog. Event Storm derartig belastet werden, daß für die eigentlichen Aufgaben keine Bandbreite verbleibt. Daher müssen solche Probleme noch vor der Notifikation behandelt werden.

2.3.4 Ereignisbehandlung

Nachdem die vorgenannten Schritte erledigt sind, sollte das Ereignis behandelt werden. Im einfachsten Fall geschieht das durch Kenntnisnahme (Acknowledgement) des Verwalters. Ist das Ereignis eine Fehlermeldung, müssen ggf. Schritte zum Beheben des Fehlers unternommen werden.

2.3.4.1 Problemdiagnose

Mit Unterstützung der im Abschnitt 2.1.3 besprochenen Help-Desk-Datenbank soll ein aufgetretenes Problem diagnostiziert werden. Entweder kann das Managementtool bereits aufgrund des Fehlers eine Diagnose stellen, oder sie muß interaktiv am Help Desk oder in der Fachabteilung getroffen werden. In jedem Fall muß aber das Ergebnis der Diagnose dem Tool bekanntgemacht werden, um damit die Wissensbasis zu erweitern.

2.3.4.2 Problemlösung

Bei der Problemlösung können Werkzeuge unterstützend wirken, indem eindeutig identifizierte Probleme automatisch behandelt werden. So könnte z. B. bei Ausfall einer Festplatte direkt ein Techniker per Pager oder Telephon benachrichtigt, bei Stopp eines Prozesses dieser automatisch wieder gestartet werden.[16]

Bei den weitaus meisten Problemen wird eine manuelle Aktion notwendig sein. Das Ziel ist, bereits am Help Desk viele der Probleme abschließend zu behandeln. Dazu wird das Werkzeug die Mitarbeiter am Help Desk, die nicht so spezialisiert sind wie die Administratoren, zum Problem führen und Lösungen aus der Wissensdatenbank anbieten. Die resultierenden Manipulationen an Systemen oder Geräten erfolgen direkt aus dem Werkzeug heraus.

---

[16] Natürlich ist davon auszugehen, daß am Prozeß ein Fehlverhalten vorliegt, wenn er stoppt. Daher muß die Anzahl der Neustarts begrenzt werden. Danach gibt das System auf und benachrichtigt einen Administrator.

Ist das Problem zu komplex, um am Help Desk bearbeitet zu werden, wird es an die zweite Ebene weitergereicht und dort behandelt.

2.4 Offenheit gegenüber anderen Systemen

Ein häufig gebrachter Einwand gegenüber umfassenden Systemen, wie sie hier besprochen werden, ist, daß sich diese Idee sehr gut eigne, wenn ein von Grund auf neues IT-System implementiert wird. Bei bestehenden Installationen sei die Heterogenität allerdings so hoch, daß kein System jede (proprietäre) Hardware gut genug verwalten könne. Dies ist nicht von der Hand zu weisen. Dennoch kann unter Mitwirkung aller Hersteller ein modulares System funktionieren. Ähnlich dem Modell von Microsoft Windows[17] wird durch Schnittstellen von der tatsächlichen Hard- oder Software abstrahiert und so die Steuerbarkeit jedes vorhandenen Objektes erreicht.

Allerdings gibt es derzeit am Markt kein Managementprodukt, welches einen umfassenden Ansatz vertritt. Computer Associates verfolgte zu Beginn der Entwicklung von Unicenter TNG einen solchen Ansatz. Es stellte sich allerdings heraus, daß der Markt nicht bereit war, den naturgemäß recht hohen Preis dafür zu zahlen. Der Grund liegt einfach im Management der Unternehmen. Es wurde in Hardware und Software zur Verwaltung des IT-Systems investiert. Weiter wurde Schulungsaufwand betrieben, um entsprechendes Know-how zu erwerben. Letztlich tritt nach Ablauf eines Anwendungszeitraumes ein Gewöhnungseffekt ein. Das hat zur Folge, daß ein neues Produkt, selbst wenn es alle Bereiche des Enterprise-IT-Management abdecken könnte, am Markt keine Chance hätte, wie 1993 an CA zu sehen war [Gro98]. Damit wird für die Hersteller von Werkzeugen zum Enterprise-IT-Management die Offenheit des Produktes ein zentrales Verkaufsargument.

---

[17] Natürlich gibt es noch eine Reihe anderer Betriebssysteme, die auch von der Hardware abstrahieren, Windows wurde nur aufgrund seiner hohen Verbreitung als Beispiel gewählt.

Dies wird zunächst erreicht, indem die Software zum Enterprise-IT-Management mit offenen Schnittstellen versehen wird, über die – so sie in Managementwerkzeugen anderer Hersteller implementiert werden – nahezu jede beliebige Applikation eingebunden werden kann. Software neueren Datums ist in aller Regel bereits mit solchen Schnittstellen versehen, so daß eine Integration in Enterprise-IT-Management-Software problemarm möglich ist. Hierzu ist allerdings zu bemerken, daß die Integration solcher Produkte eher trivial ist, da bei der Konzeption neuer Software die Offenheit eine große Rolle spielt und die Planung eines Enterprise-IT-Management durch den Hersteller des Produktes engagiert begleitet wird. Dabei kann Einfluß sowohl auf den Kunden, als auch auf den Fremdhersteller ausgeübt werden.

Wesentlich interessanter ist der Versuch, die im Unternehmen vorhandenen Managementwerkzeuge in das Produkt zu integrieren. Dazu werden bei der Installation beim Kunden Schnittstellen angepaßt und teilweise sogar neue Schnittstellen implementiert. Dieser Aufwand entsteht dadurch, daß die seit Jahren eingesetzten Managementwerkzeuge in aller Regel nicht über Schnittstellen zur Integration in ein Enterprise-Konzept verfügen und somit lediglich im Menü des Produktes zum Enterprise-IT-Management verankert werden können. Das reicht in den meisten Fällen aber nicht aus, und so werden die angesprochenen Programmiertätigkeiten notwendig.

3 Enterprise-IT-Management

Im vorangehenden Abschnitt wurden alle Tätigkeiten definiert, die zur Administration eines IT-Systems notwendig sind. Dieser Abschnitt wird der Implementierung eines Werkzeuges zum Enterprise-IT-Management, welches alle definierten Aufgaben einschließt, gewidmet.

In jeder größeren Installation wird bereits Enterprise-IT-Management betrieben, wenn auch nicht integriert in ein einzelnes Werkzeug. Die übergeordnete Instanz, die die Ergebnisse der derzeit eingesetzten Werkzeuge entgegennimmt und Aufgaben an die Werkzeuge verteilt, ist der Mensch. Dazu bedarf es hochqualifizierter Mitarbeiter, die natürlich sehr teuer sind und letztlich administrative Fähigkeiten eines Werkzeugs „emulieren“, die für die Automatisierung geradezu prädestiniert sind. Wenn also von einem Tool zum Enterprise-IT-Management die Rede ist, so muß dieses alle o. g. Aufgaben unterstützen und integrieren, soweit dies technisch möglich ist.

Im weiteren wird dann anhand einer konkreten Installation überprüft, welche administrativen Voraussetzungen geschaffen werden müssen, um einen solchen unternehmensweiten Ansatz überhaupt verfolgen zu können.

3.1 Paradigmen des IT-Managements

Zwei Wege ermöglichen den Zugang zum Enterprise-IT-Management, ein *funktionaler* und ein *objektorientierter*. Während man bisher stets den funktionalen Ansatz wählte und auch alle Werkzeuge zum Enterprise-IT-Management bzw. Netzwerkmanagement diesem Ansatz folgten, entwickeln sich einige Produkte bereits in Richtung der objektorientierten Sichtweise. Ähnlich der Entwicklung von funktionalen bzw. prozeduralen Programmiersprachen hin zu objektorientierten Programmiersprachen birgt die objektorientierte Sichtweise auf das IT-System Vorteile im Hinblick auf die Universalität.

Der objektorientierte Ansatz ist bisher in keinem der Produkte voll implementiert. Aus Zwängen, die der Markt den Herstellern auferlegt

hat, entstand ein dritter Weg, der sich zwischen funktionalem und objektorientiertem Ansatz ansiedelt und der im folgenden als „praktischer Ansatz“ bezeichnet wird. Er wird aus Marketinggründen stets als objektorientiert bezeichnet, durchbricht aber an einigen Stellen Forderungen des objektorientierten Paradigmas.

3.1.1 Funktionaler Ansatz

Ausgehend von einer funktionalen Betrachtung können die in Abschnitt 2 benannten Tätigkeitsfelder zugrundegelegt werden, um für jedes einzelne davon alle denkbaren Operationen aufzulisten. Daraus entstünde eine vollständige Beschreibung der erwünschten Funktionalität. Das Problem an dieser Herangehensweise ist jedoch, daß unmöglich alle Operationen erfaßt werden. Speziell Operationen, die bisher noch nicht notwendig waren oder technisch derzeit nicht durchführbar sind, werden nicht berücksichtigt. Neue Funktionalitäten von Geräten im IT-System können dann eventuell nicht genutzt werden. Ein Vorteil dieser Herangehensweise ist ein im Ergebnis schlankes System, da eben nicht alles Erdenkliche modelliert wird, sondern lediglich die erwarteten Funktionalitäten, die sich mit dem IT-System weiterentwickeln. Auch sind die Produkte, die dem funktionalen Ansatz folgen, keine integrativen Systeme, sondern bestehen aus einer Vielzahl von einzelnen Werkzeugen, die sich im Laufe der Zeit mit den Anforderungen der Systembetreuer entwickelten. Lediglich eine gemeinsame Schnittstelle wurde hinzugefügt, so daß die Benutzung von einer zentralen Konsole aus möglich wird.

3.1.2 Objektorientierter Ansatz

Ein objektorientierter Ansatz ist demgegenüber wesentlich umfassender. Vom zugrundeliegenden Gerät oder Prozeß wird vollständig abstrahiert. Es interessiert nicht mehr, von welchem Hersteller beispielsweise die Datenbankanwendung stammt, die Steuerung erfolgt über die Eigenschaften der Klasse `Datenbank`, aus der eine konkrete Datenbank instanziiert wird. Das objektorientierte Werkzeug

integriert alle Bestandteile und deren Manipulation. Es besteht also nicht aus einzelnen Teilprogrammen, sondern lediglich aus Agenten für die jeweiligen Objekte und Managern, die mit den Agenten kommunizieren.

Die Modellierung eines solchen Systems könnte nach denselben Prinzipien erfolgen, die schon heute dem Datenbank- oder Programmdesign zugrunde liegen. Der Ansatz, wie er in [Rum91] beschrieben ist, ist allerdings viel mächtiger, und es ist kein Grund zu erkennen, warum er nicht auch in der Verwaltung von IT-Systemen Verwendung finden könnte.

Durch die Modellierung der Funktionalität übergeordneter Objekte als Summe der Funktionalitäten der Teilobjekte erhält das Objekt `IT-System` eine hohe Komplexität. Keine einzelne Person ist dann mehr in der Lage, dieses Objekt zu überschauen. Eine der Aufgaben des Werkzeugs zum Enterprise-IT-Management muß es also sein, eine Zerlegung der Objekte in Teilobjekte durchzuführen, um im Ergebnis überschaubare Teilsysteme zu erhalten, die vom Administrator behandelt werden können. Daß solche Ansätze funktionieren können, wird am Beispiel eines Hausmeisters deutlich, der im Rahmen einer Effektivitätsuntersuchung des amerikanischen Militärs für sog. Wearables den defekten Motor eines M1A1 Abrams-Panzers reparieren konnte, obwohl er eine solche Maschine sicher bisher nicht gesehen hatte [Frey98].

3.1.3 „Praktischer Ansatz“

Der objektorientierte Ansatz hat, trotz der hohen Universalität, einen entscheidenden Nachteil: jeder Anbieter von Komponenten des IT-Systems müßte sich entweder auf eine vorgegebene Anzahl von Funktionen für ein Objekt beschränken oder seine Systeme mit entsprechender Intelligenz versorgen. Ersteres kommt aus Gründen des Marktes nicht in Frage, da es die proprietären Funktionen, die als Kaufargument im Kampf um Kunden benutzt werden, unterbindet. Letzteres erfordert Investitionen von Seiten des Herstellers, um

entsprechende Soft- und Hardware zu entwickeln, was wiederum den Verkaufspreis heben würde und möglicherweise das Produkt unattraktiv macht. Genau dies wird auch als Hauptgrund für das Scheitern des Managementstandards CMIP (siehe Abschnitt 1.1.2) der ISO angesehen. Weiter tritt das im Abschnitt 2.4 bereits angesprochene Problem des Investitionsschutzes der Unternehmung auch hier in Erscheinung.

Aus diesen Gründen haben die Anbieter „objektorientierter" Managementsysteme überall dort, wo ein Behandeln der Komponenten des IT-Systems nach dem objektorientierten Paradigma nicht möglich ist – sei es durch Ablehnung der Kunden oder durch fehlende Unterstützung von Seiten des Herstellers – eine Integration von anderen Programmen durchgeführt, die jedoch nicht notwendigerweise mit dem Managementsystem funktional verbunden sind. Das führt dazu, daß, um eine gleiche Behandlung aller Elemente des IT-Systems durchführen zu können, auf einige Informationen, die das objektorientierte Modell zu liefern in der Lage ist, verzichtet wird. Es handelt sich dabei vornehmlich um implizite Objektinformationen wie Klassenzugehörigkeit und Verbindungen zu anderen Objekten. Während die fehlende Information der Klassenzugehörigkeit sich durch geschickte Darstellung noch verbergen läßt, sind die Tracinginformationen (Verbindung zu anderen Objekten), die implizit aus den Objekteigenschaften hervorgehen, nicht so leicht zu ersetzen. So wird beispielsweise im Produkt von CA eine Art Container aus Objekten gebildet, die zur Funktion eines Geschäftsprozesses notwendig sind. Dieser Container muß manuell gefüllt werden und arbeitet wie ein Ereignismanagementsystem – die stärkste Störung wird an den Container eskaliert. Demgegenüber wirkt die Tracingeigenschaft von WBEM (siehe Abbildung 2 und Demonstration in [WBEM1]) geradezu spielerisch leicht.

3.2 Nutzung von Synergieeffekten

Durch die Einführung eines Enterprise-IT-Management sollen Kostenvorteile entstehen bzw. große Systeme handhabbarer und

transparenter gemacht werden. In den folgenden zwei Abschnitten werden Beispiele gegeben, in welchen Fällen die Nutzung eines Enterprise-IT-Management-Werkzeugs sinnvoll erscheint. Keineswegs ist der Einsatz eines Enterprise-IT-Management-Werkzeugs immer sinnvoll. In vielen Fällen wäre der Einsatz entsprechender Programme der funktionale Overkill.

3.2.1 Beispiele für die Nutzung von Synergien

Anhand dreier praxisorientierter Beispiele soll das Zusammenwirken der einzelnen Komponenten eines vollständig implementierten Enterprise-IT-Management erläutert werden. Eine vollständige Klärung des möglichen – und gewünschten – Zusammenspiels im Enterprise-IT-Management kann lediglich anhand der vorliegenden Umgebung erfolgen.

Keines der Beispiele umfaßt alle Teile des Enterprise-IT-Management. Es gibt jedoch zentrale Teile, die stets berührt werden. Demgemäß läßt sich ableiten, daß gerade diese Teile zuerst und besonders sorgfältig implementiert werden müssen, um ein Zusammenspiel im Enterprise-IT-Management erst zu ermöglichen. Weiter wird stets eine umfassende Modellierung der Unternehmens-IT vorausgesetzt, ohne die eine Nutzung der Vorteile des Konzeptes nicht möglich ist.

3.2.1.1 Beispiel 1: Umstellung der Bürosoftware

Das IT-System ist ein stark dynamisches Gebilde. Soft- und Hardware entwickeln sich schnell weiter, und um alle Vorteile der neuen Entwicklung nutzen zu können, wird im Unternehmen stets versucht, neue Programme und Technologien schnell zum Einsatz zu bringen. Allgemein ist hierbei zu erwarten, daß neue Software höhere Anforderungen an die zugrundeliegende Hardware stellen wird. Bei einer Umstellung von Software sind sehr viele Teile des Enterprise-IT-Management beteiligt.

Offensichtlich ist die Beteiligung des Tätigkeitsfeldes Softwareverteilung. Interessant wird das Konzept des Enterprise-IT-Management

bei den Tätigkeiten, die im Umfeld der tatsächlichen Verteilung stattfinden.

Vor der Einführung werden allgemein die Anforderungen an Hardware und Kommunikationsstruktur festgestellt. Daher ist recht genau bekannt, welche Zielkonfiguration die in den Einsatz der neuen Software eingebundenen Komponenten des IT-Systems haben sollten. Daraus ergibt sich die Aufgabe, diese formulierten Anforderungen mit den tatsächlichen Gegebenheiten abzugleichen und im Bedarfsfalle entsprechend zu verändern. Hier könnte der Idee gefolgt werden, eine Softwareverteilung nur auf solche Systeme durchzuführen, die tatsächlich über eine geeignete Konfiguration verfügen. Diese Aufgabe läßt sich in Zusammenarbeit mit einem Tool zum Asset Management leicht automatisieren, da dort alle Konfigurationsdaten vorliegen. Problematisch ist dabei nur, daß im Unternehmen schnell viele unterschiedliche Softwareversionen vorliegen, deren produzierte Daten u. U. nicht kompatibel sind. Deshalb wird die nächste Vorgehensweise favorisiert werden.

Diese wäre, nach vorgegebenen Regeln prüfen zu lassen, ob die notwendige Konfiguration herbeigeführt werden kann. Dazu reicht eine Prüfung der Daten nur aus dem Asset Management nicht mehr aus. Vielmehr kommen Daten aus anderen Bereichen in die Betrachtung, wie dem Kabelmanagement (zur Optimierung der Kommunikationswege), dem Sicherheitsmanagement (führt eine Veränderung der Konfiguration zu Einschnitten oder sogar Brüchen im Sicherheitskonzept) oder dem Performance Monitoring und Job Scheduling (sind noch Ressourcen vorhanden, die für Serveranwendungen benutzt werden können, oder muß neue Hardware angeschafft werden). Das Asset Management hat nicht nur Bedeutung hinsichtlich der Auskunft über die aktuelle Konfiguration; bekannte Unverträglichkeiten von Hardware sowie eine Kosten/Nutzen-Analyse fließen zusätzlich in die Entscheidungen zur Neuanschaffung oder Aufrüstung nicht geeigneter IT-Komponenten ein.

Weiter sind Berührungspunkte mit dem Storage Management und dem Backup vorhanden. Es muß geprüft werden, wo die

Programmdateien und die anfallenden Daten gespeichert werden und wie die Sicherung der Daten erfolgen soll.

Letztlich müssen alle Änderungen der Enterprise Console bekannt gemacht werden, damit beim Auftreten von Fehlern die Administratoren bzw. die Betreuer am Help Desk stets über den aktuellen Zustand des IT-Systems informiert werden können.

Bisher liegen alle diese Daten in einer stark fragmentierten Form vor – verteilt über die einzelnen Datenbanken[18] in den verschiedenen Abteilungen. Eine Integration in ein Werkzeug zum Enterprise-IT-Management sorgt vornehmlich für eine starke Automatisierung der Datenpflege, so daß Inkonsistenzen unwahrscheinlicher sind, sowie für hohe Einsparungen an Arbeitszeit, die für eben diese Datenpflege sowie der Informationsbeschaffung für die mit der Umstellung betrauten Mitarbeiter aufgewendet werden müßte.[19] Einsparungen sind auch bei Investitionen in Hardware zu erwarten, da versteckte Kosten über nicht korrekte Abrechnungen entfallen.

3.2.1.2 Beispiel 2: Administrative Expansion und Konzentration

Der IT-Dienstleister stellt für ein Unternehmen die Möglichkeit zur Nutzung von Informationstechnologie bereit. Dabei hat der Kunde, sei er nun aus dem gleichen Konzern oder nicht, maßgeblichen Einfluß auf die Behandlung der IT-Infrastruktur.

Ist der Kunde finanziell gut gestellt, wird er eine Dezentralisierung der Administration fordern. Dies ist zwar recht teuer, da personalintensiv, aber die Reaktionszeiten sind – zumindest bei bisherigen Administrationsstrukturen – wesentlich kürzer. Zudem gibt es am

---

[18] Wie weiter oben bereits beschrieben, haben die evtl. vorhandenen Werkzeuge zumeist eigene abgeschlossene Datenbasen.

[19] Es steht weniger zu erwarten, daß tatsächlich Arbeitszeit eingespart wird, als daß die vorhandenen Daten sich überhaupt durch Aktualität auszeichnen. Der Betrieb des IT-Systems hat stets den Vorrang, so daß die angesprochene Datenpflege meist zurückgestellt oder überhaupt nicht durchgeführt wird.

Standort einen kompetenten Ansprechpartner, der die Mitarbeiter schulen und unterstützen kann.

Abhängig von der Konjunkturlage kann sich diese Forderung schnell umkehren. Bei schlechter Konjunkturlage wird der Kunde eine Zentralisierung der Administration wünschen, um Kosten für dezentrales Personal einzusparen. Da dieser Prozeß dynamisch mehrfach ablaufen kann, sind bei jeder Änderung einige Hindernisse zu überwinden.

Bei der Dezentralisierung muß dem Personal am entfernten Standort eine Administrationsumgebung geschaffen werden. Dazu gehört die Einrichtung der entsprechenden Managementsysteme und deren Datenbasen. Im weiteren werden sich diese Datenbasen unabhängig von der zentralen Datenbasis fortentwickeln. Das Administrationspersonal wird sich Werkzeuge schaffen, mit deren Hilfe die Verwaltung vereinfacht werden kann. Eine Reihe von speziell auf die Bedürfnisse des zu verwaltenden Standorts abgestimmten Speziallösungen und Verfahren werden entstehen und in aller Regel nicht mit denen anderer Standorte übereinstimmen.

Bei einer Zentralisierung muß nun versucht werden, die Datenbasis in die zentrale Verwaltungsstruktur einzubinden. Die Werkzeuge des Standortes müssen geprüft und ggf. an die neuen Erfordernisse angepaßt werden. Schließlich werden neue Werkzeuge geschaffen, die die Verwaltung über die nun größere Entfernung ermöglichen. Bei jeder noch so kleinen Umstrukturierung der Administration sind alle diese Tätigkeiten erneut gefordert.

Wird hingegen ein System zum Enterprise-IT-Management eingesetzt, beschränkt sich der Aufwand zur Zentralisierung und Dezentralisierung auf ein Zu- oder Abschalten einer Managementkonsole, da die Werkzeuge zum Enterprise-IT-Management die im Abschnitt 4.3.2 dargestellten Eigenschaften besitzen sollten. Die Datenbasis ist zudem stets konsistent, da alle Verwaltungseinheiten auf einen gemeinsamen Datenbestand zugreifen. Schulungen des Mitarbeiters auf spezielle Software entfallen, und der Aufwand zur Errichtung der Managementumgebung sinkt drastisch.

3.2.1.3 Beispiel 3: Problembehebung am Help Desk

Legt man als Ziel – wie bei SBS der Fall – eine abschließende Behandlung von 80 % aller gemeldeten Probleme fest, werden an die Mitarbeiter des Help Desk sehr hohe Anforderungen gestellt. Soziale Kompetenz und Kommunikationsfähigkeit sind ebenso wichtig wie ein sicheres Beherrschen der IT-Landschaft und zwar in allen Bereichen. Außerdem befinden sich die Mitarbeiter in einer Vertrauensstellung gegenüber dem Unternehmen, da sie über umfassende Rechte verfügen müssen, um Einstellungen an den Systemen vornehmen zu können, so daß auch ihre Integrität unzweifelhaft sein muß.

Sieht man einmal von der Zweifelhaftigkeit der Existenz eines Mitarbeiters mit derartigen Eigenschaften ab, kann angenommen werden, daß ein solcher Mitarbeiter aufgrund seiner Fähigkeiten sehr teuer ist. Zieht man zudem noch in Betracht, daß jeder Standort seinen eigenen Help Desk führen muß, da nur dort die Informationen über das implementierte IT-System vorliegen, wird diese Art der Nutzerbetreuung sehr aufwendig. Dies um so mehr, als daß die Mehrzahl aller auftretenden Störungen Standardprobleme umfaßt oder vom Mitarbeiter lediglich eine Eintragung in die Datenbank erfordert. Im Ergebnis wird für eine kleine Anzahl von Ereignissen ein umfassendes und entsprechend kostenintensives Know-how vorgehalten. Für den überwiegenden Teil seiner Tätigkeit ist der Mitarbeiter am Help Desk überqualifiziert und eine optimale Nutzung der menschlichen Ressourcen nicht gewährleistet. Speziellere Probleme werden ohnehin von Fachabteilungen gelöst, wo wieder ein umfassendes Know-how zur Verfügung stehen muß. Als Nebeneffekt tritt eine Reduzierung des aufgebauten Know-hows bei den Mitarbeitern am Help Desk auf, da sie, wie oben erwähnt, zumeist mit Standardproblemen konfrontiert werden.

Die Lösung des Redundanzproblems, also des Vorhandenseins verschiedener Help Desks an verschiedenen Standorten, und der Fragmentierung derer Datenbasen, liegt im Wesen des Enterprise-IT-Management. Theoretisch würde ein zentraler Help Desk genügen, da

er Zugriff auf das gesamte IT-System nehmen und damit die gemeldeten Störungen beheben kann. Ungelöst bleibt hingegen das Sicherheitsproblem. Zur effizienten Problemlösung ist eine umfassende Berechtigung des Help-Desk-Mitarbeiters unumgänglich. Bei der Nutzung eines hierarchischen Administrationskonzeptes und dessen Abbildung im Enterprise-IT-Management ist jedoch eine feinere Granulierung als bisher möglich, so daß die Anforderungen an die Vertrauenswürdigkeit des Help Desk geringer werden.

Der größte Nutzen ergibt sich allerdings durch die Verringerung der fachlichen Anforderungen an den Mitarbeiter des Help Desk sowie durch eine weitgehende Automatisierung von Arbeitsprozessen.

Wie im Abschnitt 4.2.2 näher erläutert wird, kann bei entsprechend intuitiver Gestaltung der Oberfläche in Verbindung mit einer Hilfestellung bei der Zerlegung des IT-Systems in kleine überschaubare Funktionseinheiten am Help Desk Personal zum Einsatz kommen, welches sich lediglich durch ein gutes Allgemeinwissen zum IT-System auszeichnet. Eine Zweiteilung der Problembehandlung wird erreicht. Standardprobleme und Probleme, die durch ein stark lokales Phänomen in einer Funktionseinheit geprägt sind und dadurch vergleichsweise leicht zu erkennen sind, werden direkt am Help Desk gelöst. Dabei kann der Mitarbeiter jeweils die gesamte Funktionseinheit überschauen und muß nicht erst in den einzelnen Fachabteilungen (Netzwerke, Systeme usw.) um Informationen zur aktuellen Konfiguration bitten. Probleme, die sich erst aus dem Zusammenspiel mehrerer Funktionseinheiten ergeben oder die durch das Design des IT-Systems verursacht werden, werden, da sie am Help Desk von dortigen Mitarbeitern nicht erkannt werden, an die Fachabteilungen weitergereicht. Die hochqualifizierten und teuren Spezialisten werden in den Fachabteilungen konzentriert.

Leider gibt es keine Veröffentlichungen oder Aufzeichnungen bei SBS, die eine Abschätzung der Anzahl der zu erwartenden Probleme in den jeweiligen Problemklassen erlauben. Das Verhältnis 80% zu 20% für einfach strukturierte zu komplexen Problemen erscheint jedoch durchaus plausibel.

Eine Automatisierung der Problembehandlung wird im Zusammenspiel mit dem Ereignismanagement erreicht. Elementare Ereignisse, wie der Ausfall von Hardwarekomponenten, führen zu einem automatischen Eintrag im Help Desk[20] und sofortigen Maßnahmen zur Problemlösung – im genannten Fall zur Benachrichtigung eines Technikers. Dabei kommen auch Daten aus dem Asset Management zum Einsatz, indem der Standort des ausgefallenen Gerätes festgestellt und der zuständige Techniker ermittelt werden. Das Help-Desk-Werkzeug kann seine Vorteile voll zur Geltung bringen, weil die Priorisierung nicht mehr durch Eingriffe der Administratoren oder direkte Problemannahme ausgehebelt werden kann. Die Effizienz der Mitarbeiter am Help Desk steigt, weil sie nicht mehr über so umfangreiche Kenntnisse des IT-Systems wie bisher verfügen müssen, da alle Informationen zu einer Komponente des Systems jederzeit und leicht zugänglich zur Verfügung stehen.

Ein einfacher, konkreter Störfall könnte wie folgt behandelt werden. Nach Ausfall eines Routerports an einem entfernten Standort ist die Behandlung von Anfragen an die dortige SAP-Installation ausgefallen. Im Haus sollen zur Vorbereitung einer größeren Umstellung des FiBu-Konzeptes mehrere Mitarbeiter Datensätze aus eben der SAP-Installation zusammentragen. Der Ausfall des Ports wird ziemlich schnell in der Konsole des Help-Desk-Mitarbeiters sichtbar sein, zusätzlich wird bei Eintreffen der Meldung ein Trouble Ticket eröffnet. Aus den Business Process Views des IT-Systems geht hervor, welche Komponenten des IT-Systems mitbetroffen sind, und diese werden automatisch in einer Liste gespeichert. Da nicht klar ist, welche Ursachen der Ausfall des Routerports hat, wird der zuständige Techniker über das Asset Management ermittelt und zum Standort des Routers geschickt, der ebenfalls im Asset Management gespeichert ist. Dazu braucht der Mitarbeiter lediglich die Objekteigenschaften des Routers zu sichten, da diese alle relevanten Informationen aus den einzelnen Datenbanken enthalten. Dieser Techniker soll herausfinden, wie

[20] Dieser Eintrag ist zumeist lediglich die Eröffnung eines Trouble Tickets.

schwer der Router beschädigt ist und ob ein Austausch erfolgen muß. Anschließend soll er das Kabel in einen vom Help-Desk-Mitarbeiter benannten Port umstecken, der eine Umleitung ermöglicht, die mit Hilfe des Cable Management erarbeitet wurde. Gleichzeitig werden alle Ereignisse herausgefiltert, die durch das Fehlen des SAP-Response verursacht werden, da diese IT-Komponente aus der Liste als nicht erreichbar hervorgeht. Ruft nun ein Mitarbeiter den Help Desk ob der fehlenden SAP-Unterstützung an, kann der Help Desk bereits Aussagen über die Ursache und die voraussichtliche Dauer der Störung geben, da bei dem Versuch, ein Trouble Ticket für diese Anwendung zu eröffnen, der Hinweis auf die bereits bekannte Störung erfolgt. Der Techniker hat inzwischen den Router erreicht, das Kabel umgesteckt und das Trouble Ticket gelöst. Damit arbeitet die SAP-Anwendung wieder. Die Änderungen sind automatisch dokumentiert, da alle Änderungen an der Konfiguration über die Managementanwendung erfolgten. Der Router wird, so nicht ein größerer Schaden vorliegt, weiterbenutzt. In den Eigenschaften des Routers wird der ausgefallene Port jedoch festgehalten, damit im weiteren dieser Port, z. B. im Cable Management, nicht mehr als benutzbar zur Verfügung steht.

Bei der herkömmlichen Bearbeitung dieses Störfalles wären eine große Anzahl von manuellen Suchaktionen (wo steht der Router, wer ist der zuständige Techniker) und Dokumentationen erforderlich. Sicherlich würde, bei entsprechend umfangreichem Wissen der Administratoren, die Lösung auch gelingen, aber über Standortgrenzen hinweg würde sie zumindest länger dauern.

3.2.2 Einsparungspotentiale

Das Enterprise-IT-Management ist nicht in der Lage, für jedes Problem die optimale Lösung zu bieten. Für kleinere Installationen kann es sogar eine Verschlechterung bedeuten, wenn das Konzept mit Hilfe eines computergestützten Managementsystems verwirklicht würde. Jedes Produkt erfordert einen hohen Aufwand an

Konfiguration und Pflege, der in einem kleinen IT-System schnell den Nutzeffekt übersteigen kann.

In großen und speziell in geographisch weit verteilten IT-Systemen kann bei Einsatz eines der beschriebenen Werkzeuge an mindestens drei Stellen eine Kostensenkung erreicht werden. Erstens sinken die Personalkosten, weil eine geringere Zahl hochqualifizierter Spezialisten benötigt wird. Zweitens nehmen Wege- bzw. Transportkosten von Personal bzw. Material ab. Dieser Effekt wird allerdings durch den erhöhten Anfall von Kommunikationskosten geschmälert. Drittens sinken die Kosten, die durch den Ausfall des IT-Systems oder seiner Teile verursacht werden, und dies ist das Hauptargument für den Einsatz von Enterprise-IT-Management.

Die erste Kostensenkung ist unpopulär, weil sie auf den ersten Blick Arbeitsplätze vernichtet. Obwohl diese Vermutung richtig scheint, ist ihr doch zu widersprechen. Zwar ist zu einer gegebenen Komplexität und Heterogenität des IT-Systems eine im Verhältnis geringere Zahl hochqualifizierter Spezialisten nötig, dieser Trend hält jedoch unabhängig von den hier besprochenen Werkzeugen schon seit Einführung von Minicomputern an. Trotzdem steigt die Zahl der Arbeitsplätze, weil eine der Folgen dieser Einsparung eine ständige Erhöhung von Komplexität und Heterogenität ist. Allerdings wird die geographische Verteilung der Administration des IT-Systems stark eingeschränkt. Idealerweise gipfelt dieser Prozeß in der Konzentration der unternehmensweiten IT-Administration an einer Stelle wie es bei einigen Unternehmen bereits der Fall ist.

Da der „Remote-Schraubendreher“ noch nicht erfunden wurde, erfordern einige Tätigkeiten die physische Anwesenheit eines Administrators. Der Großteil aller täglichen Aufgaben ist aber genauso gut von einer anderen Stelle des IT-Systems möglich, wenn die entsprechenden Werkzeuge zur Verfügung stehen. Vor allem gilt, daß Tätigkeiten, die – um bei dem Eingangsbild zu bleiben – einen Schraubendreher erfordern, in aller Regel nicht von hochqualifizierten Administratoren durchgeführt werden. Zu diesem Zweck werden spezialisierte und natürlich billigere Techniker eingesetzt.

3.3 Topologie eines Firmennetzwerkes

Als Beispiel, wie ein gegebenes System verändert werden muß, um ein Enterprise-IT-Management zu ermöglichen, wird das bestehende IT-System der Firma SBS GmbH & Co. OHG im Administrationsbereich CS West (Nordrhein-Westfalen) herangezogen. Das Netzwerk ist vollständig als TCP/IP-Netzwerk ausgeführt. Die Authentifizierung erfolgt ausnahmslos über WindowsNT Server.

3.3.1 Hauptmerkmal Domänenzugehörigkeit

Das Netzwerk unterteilt sich in eine große Anzahl von WindowsNT Domänen. Teilweise ist dies durch den Einsatz von SMS bedingt, teilweise aber auch durch Anforderungen der Kunden. Seit erkannt wurde, daß die Strukturierung des Netzwerkes zentral erfolgen sollte, wird die Anzahl der Domänen verringert. Ziel ist es, pro Standort eine Domäne zu erhalten, die von einem zentralen Server aus kontrolliert wird. In jeder Domäne gibt es einen primären Server, der die Authentifizierung der Benutzer durchführt. Meist sind diesem ein oder mehrere sekundäre Server zugeordnet, die unter Nutzung der Datenbank des primären Servers zu dessen Unterstützung bei starken Lastzuständen Authentifizierungsaufgaben übernehmen.

Die derzeitige Struktur sieht vor, daß jeder Nutzer in den gewünschten Domänen ein Konto erhält. Um dies zu gewährleisten, muß er an den entsprechenden Domänen-Controllern eingetragen werden. Bei einer Änderung von Eigenschaften eines der Konten können diese nicht synchronisiert werden, sondern müssen alle manuell nachgearbeitet werden. Nach Abschluß der Reduzierungsarbeiten bei den Domänen wird zwar eine standortweite Authentifizierung durchgeführt, eine Anmeldung über Standorte hinweg ist aber nicht möglich. WindowsNT ist derzeit nicht in der Lage, eine zentrale Authentifizierung in großen strukturierten Umgebungen durchzuführen. Daher erfolgt die Administration lokal, d. h. die Benutzerkontendatenbanken der meisten Domänen liegen am dortigen Domänen-Controller vor. Einige Domänen wurden wegen administrativer Erfordernisse mit Trusts

zu anderen Domänen konfiguriert. In etwa stellt sich die Situation wie in Abbildung 9 gezeigt dar.

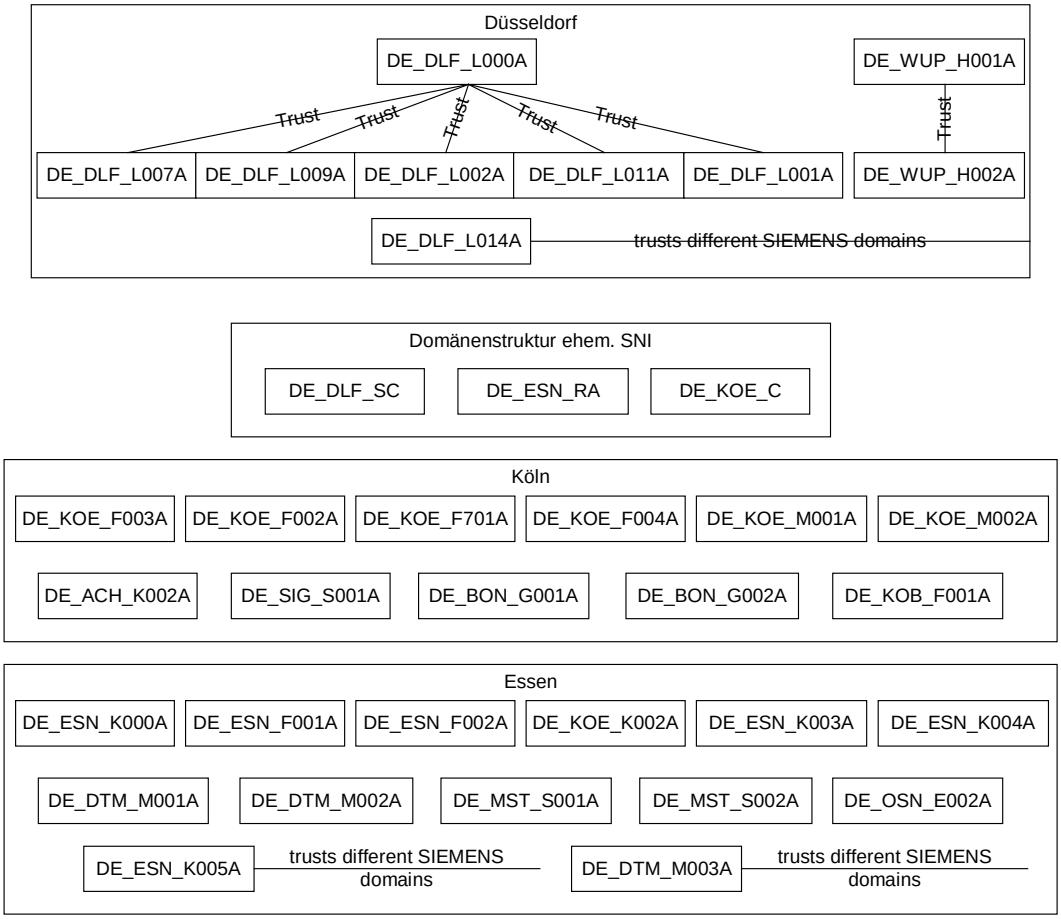

Abbildung 9: Domänenstruktur NRW nach Administrationsstandorten

Von den 36 gezeigten Domänen sind 16 aufgrund von Softwareerfordernissen zwingend notwendig. Diese enthalten jedoch keine umfangreichen Benutzerinformationen. Es bleiben also 20 Benutzerdatenbanken, die gepflegt werden müssen. Hiervon entfallen weitere 6 durch die Konfiguration von Trusts, so daß 14 unabhängige Benutzerdatenbanken gepflegt und konsistent gehalten werden.

3.3.2 Hauptmerkmal LAN/WAN-Anbindung

Aus der geschichtlichen Entwicklung des Unternehmens resultiert die Aufteilung in vier Hauptstandorte im Bereich Nordrhein-Westfalen, von denen jeder einige Nebenstandorte betreut. An den Nebenstandorten gibt es keine Administratoren. Die Administration teilt sich auf die Hauptstandorte auf. Entsprechend des am Standort anfallenden Arbeitsaufwandes ist die Netzstruktur der einzelnen Standorte unterschiedlich weit entwickelt. Die Entwicklung führt in Richtung Switched Ethernet. Der prinzipielle Aufbau ist in Abbildung 10 dargestellt, wobei die speziellen Konfigurationen nicht weiter interessieren.

Nebenstandorte sind entweder über Standleitungen an Hauptstandorte oder direkt an das SCN (Siemens Corporate Network) angebunden. Einige der Nebenstandorte sind schmalbandig an Hauptstandorte angebunden, und die Hauptstandorte wiederum sind an beide Backbone-Netzwerke angeschlossen. Diese Struktur ist gewachsen und kann nicht leicht verändert werden. Dies ist auch nicht notwendig. Die Managementsysteme können diese komplexe Struktur abbilden, und für das Management der Umgebung sind die Kommunikationswege eher nachrangig. Eine umfassende Netzstruktur ist leider nicht dokumentiert, aber auch aus dieser Prinzipdarstellung wird deutlich, daß ein Kabelmanagement mit umfangreicher Routingdokumentation das Management erheblich unterstützen kann.

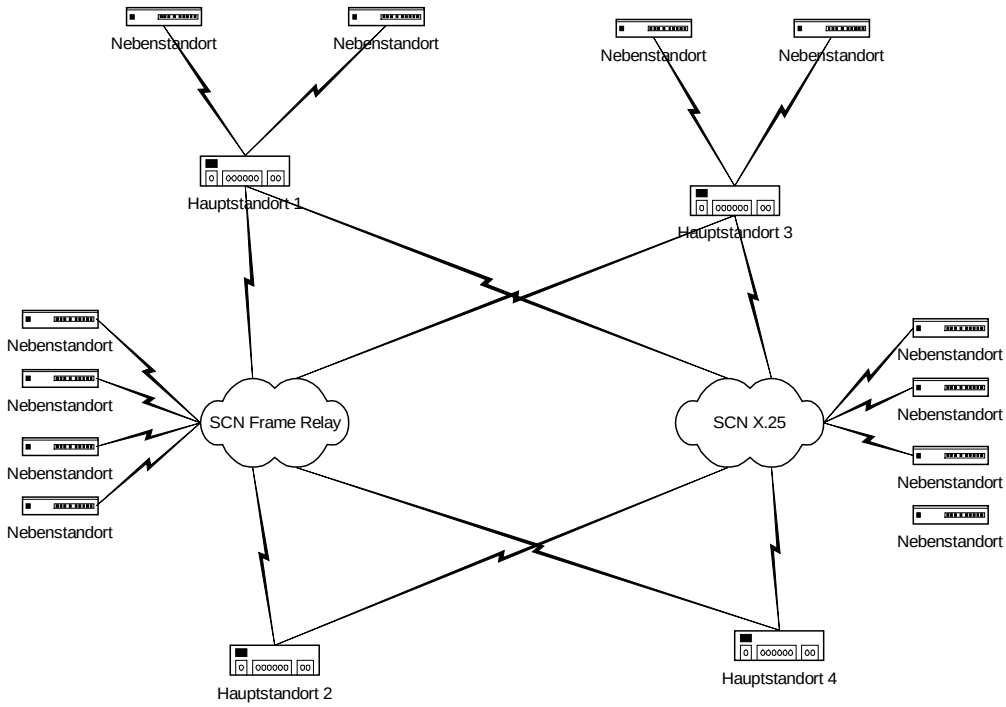

Abbildung 10: Prinzipielle Struktur des SBS-Netzwerkes

3.4 Hierarchische Administrationsstufen

Um den Einsatz eines Werkzeugs zum Enterprise-IT-Management zu ermöglichen, muß die vorhandene Administrationsstruktur verändert werden. In einem Manager-of-Manager-Konzept müssen die Datenströme je nach Bedarf immer weiter korreliert oder eskaliert werden, damit die automatische Bearbeitung der Ereignisse möglichst lokal bleibt, manuelle Aktionen aber theoretisch von jeder Konsole aus durchführbar sind. Dies erfordert jedoch ein völlig verändertes Konzept der Vertrauensstellung von den Servern des Unternehmens untereinander. Insbesondere muß es möglich sein, daß sich die Administratoren standortübergreifend an den entsprechenden Rechnern anmelden können. Der Einsatz der Version 4 von WindowsNT verhindert dieses, da nur einfachste Domänenstrukturen geschaffen werden können [Koch97].

Mit Erscheinen der neuen Version von WindowsNT – voraussichtlich im Jahr 2000 – soll dieser Mangel der bisherigen Versionen behoben werden. Leider gab es dazu bisher nur Absichtserklärungen. In der zur Verfügung stehenden Betaversion war diese Funktionalität noch nicht vollständig implementiert, so daß keine Aussagen über deren tatsächliche Nutzbarkeit gemacht werden können. Die Domänenstellung zueinander ist dann wie in Abbildung 11 gezeigt, was als Nebeneffekt den Aufwand der Administration massiv verringern würde.

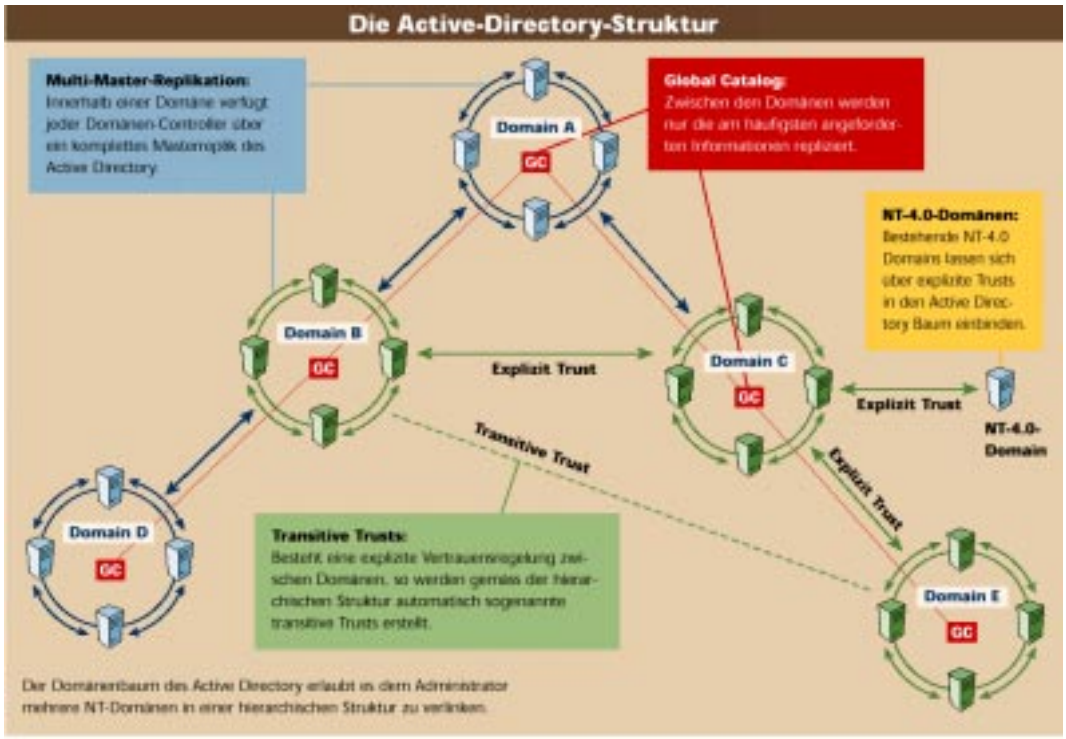

Abbildung 11: Vereinfachung der Domänenverwaltung durch Strukturierung der Domänen [Kup98]

Diese wiederum könnte im Unterschied zu Abbildung 9 mit dem neuen Konzept hierarchisch in einem Directory angeordnet werden, so daß man die bereits angesprochene Granulierung der Administration verwirklichen könnte.

Diese Struktur, wie in Abbildung 12 prinzipiell dargestellt, kann dann nicht nur Daten über Zugriffsrechte enthalten, sondern könnte auch gleichzeitig zur Personalverwaltung genutzt werden. Ein Vorteil

dieser Herangehensweise ist eine ständige Konsistenz der Datenbanken von Personalabteilung und Benutzerverwaltung an den Standorten. Die Einschränkung der Benutzer auf für sie zugängliche Maschinen erfolgt dann nicht mehr hauptsächlich über ihren Standort, sondern es können beliebige – auch entfernte – IT-Komponenten in die Berechtigungen eingetragen werden.

3.5 Hardwarekonzeption

Neben den administrativen Veränderungen, die notwendig werden, muß auch der eingesetzten Hardware Beachtung geschenkt werden. Um den Einsatz von Werkzeugen zum Enterprise-IT-Management zu ermöglichen, müssen alle zu verwaltenden Stationen über die entsprechende Ausstattung verfügen, da andernfalls möglicherweise keine hinreichenden Informationen über das zu verwaltende System vorliegen. Die Hardwareproblematik ist dabei deshalb so stark zu betonen, weil Software unproblematischer zum Einsatz gebracht werden kann und gegen Software meist auch kaum Einwände der Kunden bestehen.

Bei den Hardwarekomponenten des IT-Systems ist die Situation anders. Die für den Dienstleister selbst bereitgestellten Hardwaresysteme sind dabei der unkritische Teil. Der Nutzen kommt dem Dienstleister zugute, und er wird Anstrengungen unternehmen, Vorzüge der computerbasierten Verwaltung zu nutzen. Dazu ist er bereit, Investitionen in zusätzliche oder besser ausgestattete Hardware zu tätigen. Der Kunde hingegen profitiert nur mittelbar von der besseren Verwaltbarkeit des IT-Systems, indem die Kosten für die IT-Dienstleistung langfristig fallen. Weil der Nutzen nicht direkt sichtbar wird, überwiegt für den Betrachter aus Kundensicht der direkte Nutzen, der durch Einsparungen bei unabhängiger Beschaffung von Hardware erzielt werden kann. Deshalb wird sich der Kunde gegen die grundsätzliche Spezifikation von Hardware durch den Dienstleistungsanbieter wehren.

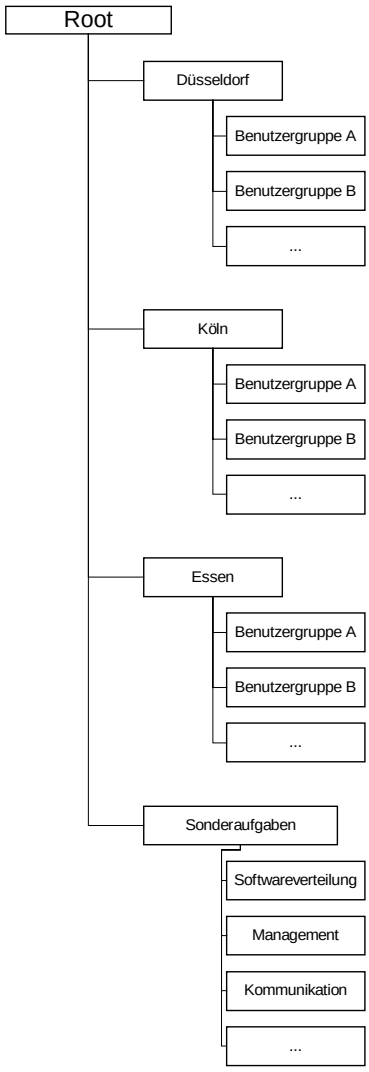

Abbildung 12: Hierarchische Neuordnung der Benutzer

Wird also ein End-to-End-Management über das gesamte IT-System angestrebt, muß ein Mittelweg gefunden werden, indem z. B. Merkmale der zu verwendenden Hardware festgeschrieben werden, wenn eine Nutzung der angebotenen Services vertraglich vereinbart wird. Das ist bei SBS bisher nicht der Fall, obwohl die Situation hier noch relativ günstig wäre, weil die verwendeten Endgeräte größtenteils vom Inhouse-Anbieter stammen. Die Bereitstellung des Service endet aber bisher vertragsgemäß an der Anschlußdose des jeweiligen

Mitarbeiters und bezieht den Arbeitsplatzrechner nicht mit ein. Wenn man aber bedenkt, welchen großen Anteil die Endgeräte am – und damit auch an den Fehlerfällen im – IT-System tragen, ist nicht einzusehen, warum gerade diese nicht mit in das Management einbezogen werden sollen. Eine Begründung mit der Tatsache, daß man die Voraussetzung mit dem Kunden nicht schaffen kann, scheint zu schwach.

3.6 Mehraufwand in Hardware

Um ein umfassendes Management der IT zu gewährleisten, wird Hardware benötigt, deren einzige Aufgabe in der Unterstützung des Managements liegt. Diese Hardware kann nicht – oder nur in kleineren Installationen in geringem Umfang – anderweitig genutzt werden. Im Hinblick darauf, daß die Anschaffungskosten von Hardwaresystemen im Vergleich zu den laufenden Kosten als gering einzustufen sind, kann die Anschaffung der zusätzlichen Hardware im Vergleich zu ihrem Nutzen vernachlässigt werden. Dem zum Betrieb der Hardware benötigten Wissen kommt demgegenüber größere Bedeutung zu.

3.6.1 Arbeitslast der Server

Der Server ist derjenige Rechner, auf dem die Serveranwendung läuft. Bei Software, die über ein Framework verfügt (siehe Abschnitt 3.1.3), ist dies derjenige Rechner, auf dem das Framework mit dem Repository und das Ereignismanagement laufen. Bei Software nach dem funktionalen Ansatz (siehe Abschnitt 3.1.1) ist nicht allgemein festzustellen, welche Teile als Server- und welche als Clientanwendung einzustufen sind. Das hängt von der jeweiligen Funktionaleinheit ab. In jedem Fall aber ist die nach dem Client/ Server-Modell geltende Definition für Serveranwendungen zugrundezulegen.

Abhängig von der Größe des zu verwaltenden Umfeldes und dem Umfang der Verwaltung fallen unterschiedlich viele Daten an. Aus der Betrachtung im Abschnitt 3.2.2 geht jedoch hervor, daß nur in großen, stark verteilten Systemen der größte Nutzen aus dem Einsatz von

Enterprise-IT-Management gezogen werden kann. Bei der Bearbeitung großer Installationen ist der Aufwand an der Servermaschine hoch, so daß ein eigens dafür zuständiger Rechner benutzt werden muß. Bei Versuchen verzögerte die Bearbeitung eines Repository über ein Class-C-Netz Anfragen an den Server auf einem Pentium-Rechner um bis zu zwei Sekunden.

Ein weiterer Aspekt ist die Verfügbarkeit der Managementsysteme für die im Unternehmen vorhandenen Plattformen. Die Problematik wurde bereits mehrfach angesprochen. Wenn ein Managementwerkzeug hinsichtlich seiner Funktionalität als geeignet eingeschätzt wird und gerade dieses Werkzeug nicht auf einer der vorhandenen Plattformen läuft, kann im Serverbereich auch Mehraufwand durch die Anschaffung neuer Serversysteme entstehen.

3.6.2 Arbeitslast der Clients

Unter Client wird hier derjenige Rechner verstanden, auf dem die Client-Applikation (Agenten und/oder Präsentationsmodule) aus Sicht des Enterprise-IT-Management-Tools laufen. Das können, im Falle von Agenten, z. B. durchaus Datenbankserver sein.

Interaktive Komponenten wie die Präsentationsmodule der Managementwerkzeuge haben in aller Regel kein Lastproblem. Da die Geschwindigkeit, mit der der Mensch mit diesen Systemen kommuniziert, weit unter der Verarbeitungsgeschwindigkeit der dafür benutzten Rechner liegt, kann eine Betrachtung dieses Problems entfallen.

Anders stellt sich die Situation bei den Teilen des IT-Systems dar, die reine Verarbeitungsleistung zur Verfügung stellen, wie z. B. Datenbankserver oder Authentifizierungsserver. Die Last dieser Systeme erhöht sich um den Betrag des Arbeitsaufwandes des Agenten. Es muß also darauf geachtet werden, daß die zusätzliche Belastung die eigentlichen Aufgaben des Rechners nicht in Mitleidenschaft zieht. Die konkrete Lastsituation hängt zu stark vom konkreten Problem ab, als daß allgemeine Aussagen möglich sind, welche zusätzliche Rechenleistung benötigt wird. Unstrittig ist aber die Tatsache, daß auf den Geräten

durch die Agenten eine höhere Last erzeugt wird und demgemäß eine höhere Leistungsfähigkeit der Geräte erforderlich ist.

3.6.3 Hardwareagenten

Hardwareagenten sind die beste, aber auch kostspieligste Lösung und zudem nicht überall einsetzbar. Sie eignen sich besonders zur Überwachung anderer Hardware sowie von Packeten im Netzwerk. Einsatzgebiete haben sie überall dort, wo Softwarelösungen die eigentliche Aufgabe der Komponente des IT-Systems beeinträchtigen würden oder nicht geeignet sind, die Überwachung vorzunehmen. Zwei Beispiele sollen das verdeutlichen.

Neben den eigentlichen Sende- und Empfangsvorrichtungen für die über das Netzwerk übertragenen Daten spielt die Qualität und der Zustand der verwendeten Kabel eine elementare Rolle bei der Herstellung von Datenverkehr. Software kann diese Qualität nicht beurteilen. Sie kann nur feststellen, ob und ggf. wo Probleme bei der Übertragung auftreten, indem sie fehlerhaft übertragene Daten zählt. Bei der Fehleranalyse ist es von entscheidendem Vorteil, Informationen über die Qualität des Mediums zu erhalten. Dazu eignen sich Hardwareagenten, die die Signale auf dem Medium auswerten, ohne sie zu verändern oder zu verarbeiten. Sie prüfen je nach Umfang der erwarteten Information z. B. die Signale hinsichtlich ihrer korrekten Modulation, den Kabelwiderstand, korrekte Terminierung und Einstreuungen von Magnetfeldern und geben damit stets Aufschluß über den Zustand. Sie generieren ein Ereignis und leiten dieses an die Managementanwendung weiter, wenn Parameter des Mediums außerhalb vorher angegebener Grenzwerte liegen. Damit kann die manuelle Suche nach Kabelproblemen bei Auftreten eines Fehlers vermieden werden.

Ein recht einfaches Beispiel für den Einsatz von Hardwareagenten wäre auch die Überwachung der aktuellen Drehzahl eines Lüfters. Da der Lüftermotor nicht um seine aktuelle Drehzahl weiß (selbst wenn er darüber Auskunft gäbe, müßte man ihn mittels Software ständig abfragen, also pollen, was eine dramatische Verschlechterung der

Systemleistung nach sich ziehen kann), liegt es nahe, ein Zusatzgerät zu installieren, welches die Drehzahl am Lüfter abgreift und bei Abweichung der Drehzahl von vorher festgelegten Maßgaben ein Ereignis auslöst. Damit filtert der Agent bereits einen Teil der Ereignisse, was die Managementsoftware und damit den Client-Rechner entlastet.

3.7 Betrachtungen zum Kommunikationsaufwand

Auch wenn die Kommunikation der Teile eines Werkzeuges zum Enterprise-IT-Management teilweise verbindungslos stattfindet, erzeugt der Einsatz eines solchen Programms stets Verkehr auf den Leitungen des Unternehmens. In den nächsten Abschnitten wird sich zeigen, daß diese zusätzliche Belastung unumgänglich und in den meisten Fällen nicht relevant ist. Trotzdem kann in extremen Fällen, insbesondere durch fehlerhaftes Design, dieser Datenfluß den Nutzdatenverkehr übersteigen oder das Netzwerk zum Zusammenbruch bringen. Es ist deshalb wichtig, die benötigten Informationen sehr genau zu spezifizieren und die verteilte Umgebung sorgfältig zu modellieren. Das gilt auch dann, wenn vermeintlich eine ausreichende Bandbreite zur Verfügung steht, da erstens jeder Traffic Kosten verursacht und zweitens einmal verschenkte Bandbreite nicht mehr anderweitig verwendet werden kann und somit eine optimale Nutzung der IT-Ressourcen nicht erfolgt.

3.7.1 Kommunikationskosten

Jede zusätzlich in das IT-System eingebrachte Client/Server-Anwendung bedeutet Verkehr auf der Netzwerkinfrastruktur. Wenn dies einem offensichtlich produktiven Ziel im Sinne des Kerngeschäftes des IT-Dienstleisters dient, also etwa der Bereitstellung von Speicherplatz oder der Verteilung von Software, wird die Notwendigkeit nicht angezweifelt und ggf. die Bandbreite erhöht. Anders ist die Bereitschaft, wenn es darum geht, Bandbreite zur Verwaltung des IT-Systems bereitzustellen. Dann wird eine ablehnende Haltung

eingenommen, da eine effektivere Verwaltung sich nicht in unmittelbarer Gewinnerhöhung beziffern läßt.

Dabei stellt sich die Situation nicht so dramatisch dar, wie sich vielleicht erwarten ließe. Im Versuchsaufbau mit verschiedenen Managementprodukten und deren Grundfunktionen ließ sich keine gravierende Erhöhung der Netzlast messen (siehe Tabelle 1). ManageX als Produktteil von OpenView, TransView ControlCenter und UnicenterTNG Framework wurden installiert und über längere Zeit beobachtet. Es wurden Messungen zur erzeugten Netzlast durchgeführt, insoweit dies unter dem Betriebssystem WindowsNT möglich ist.

Dabei stellte sich heraus, daß in einer Anfangsphase eine überdurchschnittlich hohe Belastung des Netzwerkes erfolgt, um die Kommunikation der Systemkomponenten untereinander zu initialisieren. Diese Verbindung nutzt die volle verfügbare Bandbreite aus, ist für den Betrieb des Systems jedoch nicht entscheidend. Im weiteren verteilt sich die Netzwerklast statistisch. Der Wertebereich liegt jeweils zwischen Null und der maximalen Bandbreite. Daher wurde ein arithmetisches Mittel über eine Meßdauer von 500 Sekunden gebildet. Angesichts der theoretisch möglichen Übertragung von rund 520 MByte in dieser Zeitspanne können die ermittelten Werte als aussagekräftig angesehen werden.

Es steht nicht zu erwarten, daß eine repräsentative Konfiguration gefunden werden kann, die allgemeine Aussagen über die zu erwartenden Netzbelastungen in einer konkreten Umgebung zuließe. Daher wurden vier Managementfunktionen ausgewählt. Die durch den Einsatz dieser Managementfunktionen entstandene Last ist in Tabelle 1 zusammengestellt.

Tabelle 1: Netzlast verschiedener Managementanwendungen

Art der Belastung	10^6 Bits/sec.	% Bandw.
Maximale Bandbreite 5 Wiederholungen	8,74	100
Remote Control Durchschnitt über 500 Sek. (pcANYWHERE)	0,037	0,42
Remote Control Durchschnitt über 500 Sek. (WinVNC)	0,41	4,73
Event Management Durchschnitt über 500 Sek., 760 Ereignisse (ManageX)	0,15	1,75
Auto Discovery Messung über ein Class A Netz, 7 Objekte (Unicenter TNG)	0,001	0,01
Remote Monitoring Durchschnitt über 500 Sek., 10 Werte (ManageX)	0,058	0,66
Remote Monitoring Durchschnitt über 500 Sek., 10 Werte (Betriebssystemfunktion)	0,070	0,80

Nicht alle Produkte konnten einzeln getestet werden, da die zur Verfügung stehenden Testversionen nicht alle Funktionen des vollständigen Produktes enthielten. Die Ergebnisse dürften sich aber nicht gravierend unterscheiden, wie an der Vergleichsmessung zum Remote Monitoring zu sehen ist. Einzig der Meßwert für Remote Control wurde mit einem sehr schmalbandigen Produkt ermittelt, welches bei der SBS über WAN zum Einsatz kommt. In diesem Punkt könnten größere Abweichungen bei Einsatz eines anderen Produktes entstehen. Der Wert der Vergleichsmessung mit einem anderen Produkt läßt darauf schließen.

3.7.2 Netzlast vs. Arbeitsleistung

Eine Vermeidung von großer Netzlast kann durch die weitgehende Verteilung der Informationsverarbeitung erfolgen. Wenn z. B. die Ereigniskorrelation an den Clients bereits erfolgt und die Ereignisse gesammelt und in komprimierten Datenblöcken an das zentrale Ereignismanagement geschickt werden, sinkt die durch die Managementanwendung verursachte Netzlast stark. Auf der anderen Seite steigt aber die Betriebslast auf dem Clientrechner an, auf dem Client

muß Speicherplatz für Datenbasen vorgehalten werden, und letztlich wird die Aktualität des zentralen Ereignismanagements herabgesetzt. Zudem leisten eine Reihe von Geräten, wie z. B. die aktiven Netzwerkkomponenten, die selbständige Vorverarbeitung der Daten derzeit nicht und müßten dahingehend erweitert werden. Der Datenverkehr bliebe auch nicht aus, sondern würde nur auf weniger verkehrsstarke Zeiten verschoben, da mit der lokalen Verarbeitung zwar im Moment weniger Verkehr auf dem Netzwerk verursacht wird, aber die Datenbasen ständig aktualisiert werden müssen.

Eine Vorverarbeitung steht der optimalen Nutzung der Clients, also den produktiven Komponenten des IT-Systems, entgegen. Daher muß die erhöhte Netzlast in Kauf genommen werden und kann nur durch intelligentes Design der verteilten Umgebung mit Serverinstanzen (siehe Abschnitt 4.3.2) reduziert werden.

3.8 Notwendigkeit von Fehlertoleranzen

Da ein Hauptbestandteil eines Managementsystems die Fehlerbehandlung ist, steht die Forderung, daß das System stabil bleibt, wenn die Verbindung zu seinen Agenten und Anzeigemodulen unterbrochen wird. Durch Wiederaufnahmealgorithmen und den Schutz der Datenbankintegrität ist dies weitgehend gewährleistet. Interessanter ist der Fall der Fehlererkennung.

Eine Mischung aus verbindungsorientierter und verbindungsloser Kommunikation stellt den sinnvollsten Weg dar. Während bei allen Datenoperationen mit dem Repository oder den entsprechenden Datenbanken eine sichere Verbindung gewährleistet sein muß (verbindungsorientiertes Protokoll), um die Integrität der Datenbanken zu wahren, ist bei der Signalisierung eines Fehlers ein verbindungsloses Protokoll effizienter. Die Motivation dieser Zweiteilung ist klar. Benachrichtigungen über Fehler im IT-System haben größere Chancen anzukommen, wenn sie verbindungslos abgesetzt werden [Rose94]. Die Zuverlässigkeit der Verbindung ist weder a priori gegeben, noch notwendig, da das IT-System ja offensichtlich schon fehlerhaft arbeitet.

Die Anforderungen eines vertrauenswürdigen, verbindungsorientierten Protokolls können die Benachrichtigung über Fehler sogar ungewollt verhindern.

3.9 Manuelle vs. automatische Aktionen

Die überwiegende Menge der auftretenden Ereignisse werden Standardprobleme sein, für die bereits Lösungswege erarbeitet wurden. Daneben wird es noch eine Reihe Ereignisse geben, die zwar nicht ständig auftreten, die aber automatisch aufgelöst werden können. Für alle diese Meldungen ist es normalerweise nötig, daß Mitarbeiter die Lösung angeben (siehe Diskussion im Abschnitt 3.2.1.3). Geht die Dokumentation der durchgeführten Schritte zur Lösung in die Betrachtung ein, so verursacht ein simples Problem einen beachtlichen Arbeitsaufwand. Hier kann die Automatisierung große Einsparungen an Arbeitszeit bringen.

Die für den Betrieb des IT-Systems verantwortlichen Mitarbeiter sehen sich in aller Regel einem starken Zeitdruck ausgesetzt. Unter diesen Voraussetzungen werden einfache Probleme sofort gelöst, ohne die notwendige Dokumentation durchzuführen. Daraus resultiert zunächst nur eine Verzerrung der Statistiken über das IT-System, wie über Zuverlässigkeit, Design, Instandhaltungskosten usw. Ein weiteres Manko schleicht sich aber ungewollt ein. Da die kleinen, einfachen Probleme sofort gelöst werden, ohne sie in die Problemliste – gleich welcher Art – einzustellen, wird eine vorhandene Problempriorisierung ausgehebelt. Kleine Probleme werden wegen ihres geringen Lösungsaufwandes bevorzugt behandelt, was die Lösung größerer, komplexerer Probleme verzögert. In der Folge gestaltet sich eine Sicherung der Funktion des IT-Systems und damit der Services, die angeboten werden, schwierig, da ein planmäßiges Vorgehen nicht mehr möglich ist, weil jeder Mitarbeiter die Priorität eines Problems nach Gutdünken festlegt.

Weitgehende Automatisierung kann einer Aufweichung der Vorgaben zur Schrittfolge bei der Problembehebung entgegenwirken.

Insbesondere ist es vorstellbar, daß bei einem ankommenden Ruf am Help Desk automatisch ein Trouble Ticket eröffnet würde und der Mitarbeiter nur über die Benutzung dieses Tickets Zugriff auf das IT-System bekäme. Neben einer automatischen Dokumentation des Problems, der zugehörigen Lösung und den dazu unternommenen Schritten würde eine Priorisierung der Probleme stets nach allgemeingültigen Regeln erfolgen.

Eingriffe in die Bearbeitung von Problemen sind nicht nötig, wenn sie vom Agenten oder Korrelationswerkzeug aufgelöst wurden. Sie können daher vollautomatisch erfolgen. Lediglich die Ereigniskonsole erhält eine Meldung über eingeleitete Maßnahmen. Dadurch ist zu erwarten, daß das Arbeitsaufkommen für die Administratoren sinkt und die Effizienz der Problemlösung bzw. des Betriebs des IT-Systems steigt.

4 Aktuelles Marktangebot

Bei der Betrachtung des aktuellen Marktangebotes ist naturgemäß keine erschöpfende Produktliste zu erwarten. Vielmehr bieten eine Reihe von Firmen Lösungen für Bereiche des vorgestellten IT-Managements an. In die vorliegende Betrachtung kamen daher nur Produkte, die aufgrund der Aussagen der Hersteller eine umfassende Unterstützung – wenn auch durch Integration von Programmen anderer Anbieter – in Aussicht stellen.

An dieser Stelle soll es keinesfalls darum gehen, eine Vollständigkeitsanalyse der Produkte hinsichtlich des weiter oben definierten IT-Managements durchzuführen.[21] Lediglich die Unterstützung der Administratoren bei der zentralen Verwaltung des IT-Systems soll dargestellt werden. Die vorliegende Arbeit versteht sich auch als zu grundsätzlich, als daß Funktionen geprüft werden könnten. Dann fielen alle am Markt angebotenen Produkte durch. Ein Beispiel für fehlende Funktionalität ist die Nutzerverwaltung. Keines der im folgenden genannten Systeme abstrahiert vom Betriebssystem und stellt eine unternehmensweite Nutzerverwaltung bereit, die plattformübergreifend Nutzerkonten anlegen, manipulieren und entfernen kann. Laut Auskunft von HP wird das sich wohl erst im nächsten Jahrtausend ändern, obwohl fieberhaft daran gearbeitet wird [Gie98].

4.1 Beteiligte Produkte

Bei den Produkten, die heute am Markt plaziert sind, gibt es zwei Grundtendenzen. Sie unterscheiden sich in der Art des Zusammenwirkens der einzelnen Komponenten des Managementsystems.

Einerseits wird ein integrativer Aufbau des Produktes angestrebt. Hierzu werden alle Aufgaben des Managements unter einer Schnittstelle, die als Framework bezeichnet wird, zusammengefaßt, also in

[21] Dies ist auch nicht gut möglich, da die Anforderungen jeder Firma anders sein können. Um hier eine ganz speziell auf die vorliegende Situation abgestimmte Analyse zu bekommen, kann man z. B. das Tool der Gartner Group Inc. verwenden.

einem einzelnen Produkt integriert. Die Kopplung der einzelnen Teile des Produktes ist demgemäß sehr eng. Dadurch kann einerseits ein hocheffektives Benutzerinterface gestaltet werden, andererseits muß bereits bei der Entwicklung neuer Komponenten für das Produkt massiv Einfluß auf die Programmierung ausgeübt werden, was die Offenheit einschränkt. *IBM* mit ihrem *Tivoli TME10*[22] und *Unicenter TNG* von *Computer Associates*[23] verfolgen diesen Ansatz. Obwohl in Marketingveranstaltungen dieser Anbieter darauf hingewiesen wird, daß ein objektorientierter Ansatz verfolgt wird, ist dies, zumindest im Sinne der Objektorientierung wie im Abschnitt 3.1 beschrieben, falsch.

Einen anderen Weg beschreiten die Produkte *OpenView* von *Hewlett Packard*[24], *SPECTRUM* von *Cabletron*[25] und *TransView* von *SIEMENS NIXDORF*[26]. Hier wird auf eine lose Kopplung ansonsten eigenständiger Programme gesetzt. Der Hauptvorteil dieser Herangehensweise besteht ganz klar in einer Verringerung des Programmieraufwandes, weil auch Programme anderer Firmen auf diese Weise leicht integrierbar sind. Der Hauptnachteil liegt in einer teilweisen Aufgabe der Durchgängigkeit, weil jedes Produktteil für sich gestaltet wird und ein einheitliches Look-and-Feel schwierig zu erreichen ist. Dies gilt insbesondere für die sog. Menüintegration, bei der lediglich ein Menüpunkt zum Aufruf der Fremdapplikation vorhanden ist, sonst aber keine Schnittstellen zwischen den Programmen bestehen.

Letzte Entwicklungen am Markt bestätigen, daß das Produkt SNI TransView nach einer Umstrukturierung der Geschäftsfelder des SIEMENS-Konzerns eingestellt wird. In der Folge wird eine Partnerschaft mit Computer Associates etabliert, in deren Produkt Unicenter

---

[22] Diese und alle weiteren Produktinformationen über Tivoli TME 10 sind entnommen aus [TME1].

[23] Diese und alle weiteren Produktinformationen über CA Unicenter TNG sind entnommen aus [TNG1], [TNG2] und [TNG3].

[24] Diese und alle weiteren Produktinformationen über Tivoli TME 10 sind entnommen aus [OV1].

[25] Diese und alle weiteren Produktinformationen über Tivoli TME 10 sind entnommen aus [Spec1].

[26] Diese und alle weiteren Produktinformationen über Tivoli TME 10 sind entnommen aus [TV1].

TNG Teile des TransView Know-hows aufgehen werden. Dafür wird SIEMENS den Vertrieb und das Marketing von Computer Associates übernehmen. Zukünftig wird es also nur noch ein Produkt dieser beiden Anbieter geben. Da bisher allerdings unklar ist, welche Eigenschaften das neue Produkt haben wird, sind in der vorliegenden Arbeit noch beide Werkzeuge beschrieben.

SPECTRUM von Cabletron ist keine eigenständige Lösung zum Enterprise-IT-Management. In Verbindung mit *Patrol* der Firma *BMC* und dem Help Desk der Firma *Remedy* kann eine Lösung zusammengestellt werden, die als Enterprise-IT-Management bezeichnet werden kann.[27] Dieses Produktpaket ist ein Beispiel dafür, daß Enterprise-IT-Management nicht vom Einsatz eines Produktes abhängig ist, sondern auch auf anderen Wegen modelliert werden kann. Da in dieser Arbeit aber die direkt für das Enterprise-IT-Management entworfenen Produkte im Mittelpunkt stehen sollen, soll es bei dieser Erwähnung bleiben.

4.2 Technische Anforderungen

Neben den Funktionen, die unterstützend bei der Lösung der im Abschnitt 2 herausgearbeiteten Aufgaben wirken, werden an ein umfassendes Werkzeug zum Enterprise-IT-Management grundlegende Anforderungen gestellt, die im folgenden erläutert werden. Dabei wird der Schwerpunkt auf die Administration einer WindowsNT-Umgebung gelegt, da zum einen das betrachtete Netzwerk bei SBS auf WindowsNT migriert und zum anderen eine Betrachtung aller Betriebssysteme den Rahmen dieser Arbeit sprengen würde.

4.2.1 Plattform

Ein homogenes IT-System mit lediglich einem Maschinentypus und einem Betriebssystem gibt es heute kaum noch. Verschiedene

[27] Weitere Informationen sind auf den Homepages der jeweiligen Hersteller BMC [BMC1] und Remedy [Rem1] zu finden.

Unix-Versionen, WindowsNT, OS/2 und Novell Netware sind die gängigsten Serverbetriebssysteme, wobei ein integriertes Managementsystem für Netware wegen der fehlenden graphischen Oberfläche ohnehin auf einem anderen System laufen müßte. In Netzwerken, deren Server hochverfügbar sein müssen, werden Rechner namhafter Hersteller verwendet. Dazu zählen IBM, Compaq, Hewlett Packard, SNI und weitere Firmen. Diese Systeme beinhalten in aller Regel bereits Managementfunktionalität und sind mit spezieller Hardware (wie z. B. ECC-Speicher) ausgerüstet.

Diese vorhandene Hardware und Software muß als Plattform dienen können. Auch das beste Werkzeug hat keinen Wert, wenn dafür spezielle Rechner und Betriebssysteme, im schlechtesten Fall noch zusätzlich, in das IT-System eingebracht werden müssen. Auch eine Reduzierung der Komplexität des IT-Systems ist möglich, weil bei durchgängiger Unterstützung auch Systeme, die nur für das Management benutzt wurden, entfallen können. Im Beispiel des betrachteten Umfeldes betrifft dies einige SUN-Workstations, die lediglich zur Verwaltung der Netzwerkgeräte dienen. Bei entsprechender Modellierung der Funktionalität auf die im Unternehmen eingesetzten WindowsNT-Systeme könnten die SUN-Rechner entfernt und damit die Heterogenität des IT-Systems verringert werden.

Der kleinste gemeinsame Nenner fast jeden größeren Netzwerkes ist WindowsNT. In kaum einem solchen System befindet sich nicht mindestens ein WindowsNT Server. So wäre zu erwarten, daß alle verfügbaren Produkte zumindest WindowsNT als Plattform unterstützen, um einer weiteren Erhöhung der Heterogenität des Netzwerkes bei Einsatz des Produktes entgegenzuwirken. Leider ist das derzeit nicht der Fall, wie im folgenden zu sehen ist. Die Begründung ist in der Geschichte dieser Systeme zu suchen. Fast alle Produkte basieren auf den Netzwerkmanagementsystemen dieser Hersteller aus den 80er Jahren. Zu dieser Zeit gab es aber als Netzwerkbetriebssystem abseits der Mainframes nur UNIX. Jeder Hersteller setzte auf seinem Unix-System auf und erstellte dafür ein Werkzeug. Mit der Zeit wurden die Werkzeuge auch auf Unix-Systeme anderer Hersteller portiert. 1993

trat WindowsNT mit einem völlig veränderten Systemansatz an. Zunächst wurde von den Administratoren dieses Betriebssystem ignoriert. Zu stark war die Bindung an die Unix-Philosophie, und auch heute noch gibt es stark emotional geführte Auseinandersetzungen, welches der beiden Konzepte besser sei. Mit der Verbreitung von WindowsNT wurden immer mehr Produkte – oder besser Produktteile – auf WindowsNT portiert. Heute hat WindowsNT ein solch starkes Wachstum genommen, daß einige Hersteller direkt für WindowsNT entwickeln und dann auf UNIX portieren [Hab98]. Allerdings liegen die Ergebnisse dieser Entwicklung zum jetzigen Zeitpunkt noch nicht vor.

TransView unterstützt drei Unix-Systeme (SNI, HP, SUN) und WindowsNT. Die Managementplattform *TransView SNMP* ist allerdings nicht für WindowsNT verfügbar, was die Möglichkeiten eines Einsatzes auf diesem Betriebssystem stark einschränkt. Letzten Auskünften des Herstellers zufolge wird TransView SNMP nicht für WindowsNT portiert, dessen Funktionalität aber in das Produkt *TransView ControlCenter*, welches ein Eventmanagement bereitstellt, integriert. Wenn das erfolgt ist, kann TransView auch als vollwertige Enterprise-IT-Management-Lösung angesehen werden. Ob dies jedoch im verbleibenden Zeitraum der Produktentwicklung von angekündigten zwei Jahren noch verwirklicht wird, darf als zweifelhaft angesehen werden.

OpenView von Hewlett Packard wird zwar für WindowsNT angeboten (Produktname *ManageX*), die Funktionalität eines Enterprise-IT-Management kann jedoch nur auf der Plattform HP-UX erreicht werden, wobei durch recht klare Vorgaben hinsichtlich der Hard- und Softwareausstattung kaum Spielraum verbleibt. ManageX selbst ist ein reines Ereignismanagement für WindowsNT ohne Funktionalitäten im Netzwerkmanagementbereich. Die einzelnen Produkte aus der OpenView-Familie sind zwar für WindowsNT verfügbar, aber die integralen Bestandteile, also die Konsolen, die die einzelnen Produkte verbinden, gibt es derzeit nicht für diese Plattform. OpenView ist daher

nur bedingt geeignet, Enterprise-IT-Management auf WindowsNT anzubieten.

Unicenter TNG kann als einziges Produkt vollständig auf WindowsNT, allerdings größtenteils nur dort, als Plattform eingesetzt werden.

TME 10 von IBM bietet eine Unterstützung von WindowsNT nur teilweise an. Das Framework, genannt *Tivoli Management Platform*, ist für WindowsNT verfügbar. Für die einzelnen Verwaltungslösungen gilt das jedoch nicht. Die Benutzerverwaltung *Tivoli/Admin* ist derzeit nicht für WindowsNT erhältlich, so daß ein Security Management unmöglich wird. Asset Management (*Tivoli/Inventory*), Softwaredistribution (*Tivoli/Courier*) und Monitoring (*Tivoli/Sentry*) können auf der Plattform WindowsNT durchgeführt werden. Das wichtigste Teil jedoch, die integrierende Enterprise-Management-Console (*Tivoli/Enterprise Console*) arbeitet derzeit nur mit diversen Unix-Betriebssystemen zusammen. Ähnlich wie HP ist es daher nur bedingt für ein Enterprise-IT-Management unter WindowsNT geeignet.

4.2.2 Benutzeroberfläche

Das Erscheinungsbild von Benutzeroberflächen erzeugt subjektive Wertungen. Allerdings nähern sich die Basiselemente moderner Produkte einander an. So besitzt heute fast jedes Betriebssystem ein graphisches Frontend mit Fenstertechnik und bestimmten Menüstrukturen. Dies ist mit einer besonderen Effektivität bestimmter Kommunikationselemente zu begründen.

An eine Benutzeroberfläche müssen folgende Anforderungen gestellt werden [Shn93]:

- Sie muß intuitiv sein, d. h. eine nicht konkret auf dieses Interface geschulte Person sollte, vorausgesetzt sie weiß, welche Funktion sie ausführen will und welche Angaben dazu evtl. nötig sein könnten, mit dem System arbeiten können.
- Sie muß effektiv sein, d. h. die Abbildung der Funktionen in Menüs und Dialogen muß dem Ablauf des Arbeitsprozesses entsprechen, besser noch der Schrittfolge, in der beim Abarbeiten einer Aufgabe von der betreffenden Person gedacht wird. Hierbei

ist vor allem auch wichtig, möglichst schnell und ohne Umwege Zugriff auf Funktionen zu bekommen.
- Sie muß Informationen und Funktionen übersichtlich und sinnvoll verknüpfen und darstellen, ohne den Benutzer mit Information zu überfrachten.

Alle Produkte verwenden graphische Frontends mit Fenstertechnik zur Darstellung der Informationen. Sie sind mit Zeigegeräten steuerbar, und der Zugriff auf die einzelnen Funktionen erfolgt über Menüs. Nur bei der Repräsentation des IT-Systems gibt es unterschiedliche Ansätze.

4.2.2.1 Zweidimensional

Alle Produkte bieten eine zweidimensionale Repräsentation des Netzwerkes an. Diese Applikation bzw. dieser Applikationsteil ist aber bei den meisten Produkten nicht auf allen Betriebssystemen verfügbar. Ein Produkt, welches universell, d. h. auf allen Plattformen einsetzbar ist, gibt es zum heutigen Zeitpunkt noch nicht.

Beim Betrachten von Abbildung 13 als Darstellung eines typischen Netzbildes fällt sofort auf, daß hier lediglich die Netzwerkkomponenten enthalten sind. Prozesse oder Geräte und deren Bauteile werden typischerweise von solchen Systemen nicht in die graphische Darstellung integriert. Für diese Komponenten gibt es eigene, von den Netzwerkkomponenten getrennte Repräsentationen. Damit erschließen sich anhand der Darstellung des IT-Systems nicht sofort die Beziehungen aller Teile des IT-Systems zueinander, wie dies z.B. im nächsten Abschnitt der Fall sein wird. Außerdem ist die geographische Verteilung nicht integriert. Für die Fehlerverfolgung speziell in stark verteilten IT-Systemen wäre das aber ein enormer und wünschenswerter Informationsgewinn.

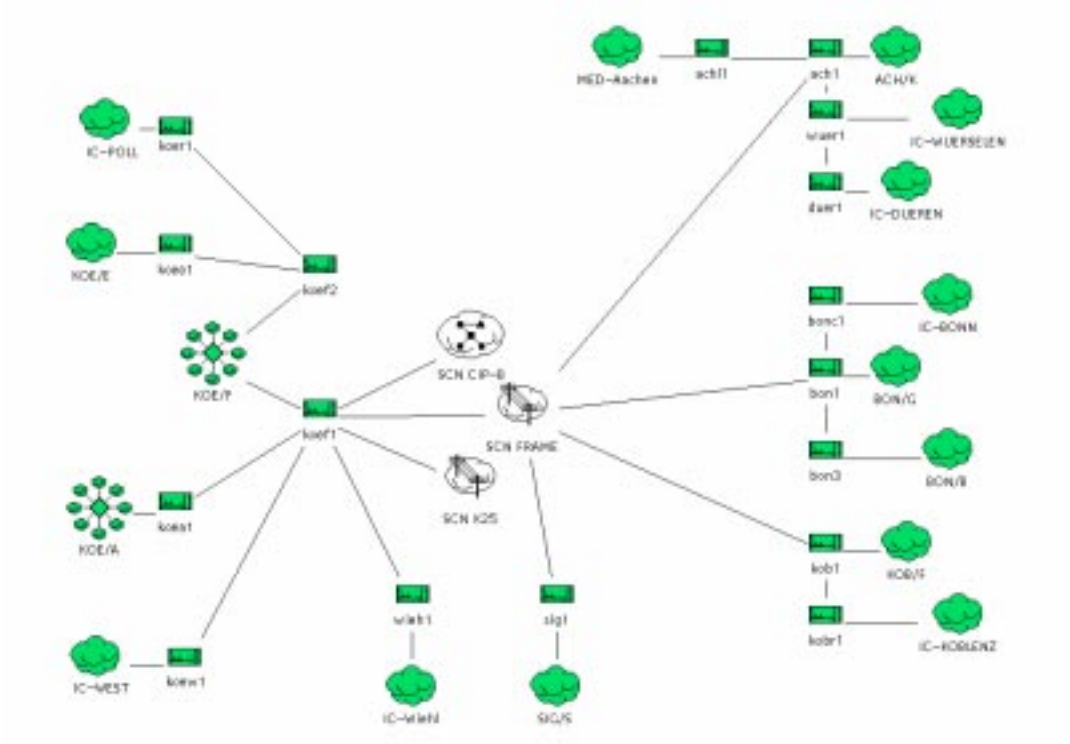

Abbildung 13: Typisches Layout einer zweidimensionalen Netzwerkrepräsentation

4.2.2.2 Dreidimensional

Ein Produkt wirbt mit einer dreidimensionalen Oberfläche – CA Unicenter TNG. Kritiker bezeichnen diese abfällig als „Videospiel“, Befürworter loben sie als neue Dimension in der intuitiven Benutzerführung.

Zunächst benötigt die Oberfläche besondere Hardware (OpenGL-fähige Graphikkarte). Ist in der Managementkonsole keine solche vorhanden, muß auf die ebenfalls vorhandene zweidimensionale Oberfläche zurückgegriffen werden. Weiter betrifft die Aussage dreidimensional lediglich die Repräsentation des IT-Systems. Diese ist allerdings sehr gelungen.

Selbst eine nicht vorgebildete Person wird sich in einer Darstellung wie in Abbildung 14 zurechtfinden und kann sich innerhalb des Unternehmensnetzwerkes bis zu einem bestimmten Gerät oder Prozeß vortasten. Dabei kommt der Darstellung zugute, daß die Sinnbilder der Geräte, Hausnetze u. dgl. ihrem natürlichen Gegenstück weitestgehend ähnlich sehen oder durch Vergleiche abstrakte Konzepte greifbarer machen (im rechten Bild wird die Festplatte durch einen Aktenschrank und ein Bücherregal repräsentiert).

Abseits der schönen farbigen Darstellung fällt an der Bedienung auf, daß auf alle Optionen, die bei einem bestimmten Netzwerkobjekt zur Verfügung stehen, über kontextsensitive Menüs komfortabel und schnell zugegriffen werden kann.

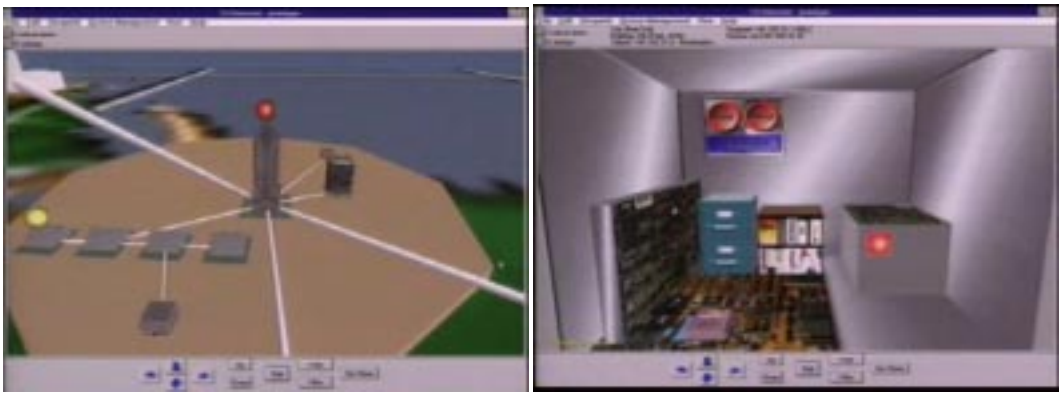

Abbildung 14: Intuitive Darstellung von Komponenten des IT-Systems [TNG4]

Laut Auskunft des Herstellers ist diese Oberfläche aber derartig pflegeintensiv, daß nur Unternehmen, die besonders innovativ erscheinen möchten, diesen Aufwand betreiben werden. Eine voll funktionale Modellierung inklusive Drag-and-Drop-Steuerung der Managementfunktionen dürfte allerdings auch deren Ressourcen erschöpfen [Gro98].

4.2.3 Kommunikationsprotokolle

Unabhängig vom konkreten Ansatz müssen die Teile der Produkte miteinander kommunizieren. Insbesondere ist zu beachten, daß ein

Teil der Kommunikation möglicherweise unter Ausnahmezuständen stattfindet. Dies ist dann der Fall, wenn eine Störung am Netzwerk vorliegt, so daß gesicherte Kommunikation nicht mehr möglich ist [Rose94]. Andererseits sind Teile wie z. B. Datenbanken derart anfällig gegenüber fehlerhaften Übertragungen, daß der unzweifelhafte Abschluß einer Operation sichergestellt werden muß. Aus diesem Grund bestehen sehr hohe Anforderungen an die Spezifikation und Implementation der Kommunikationsarchitektur.

4.2.3.1 Standardprotokolle des Netzwerkmanagements

Der einfachste und naheliegendste Weg der Kommunikation stellen Standardprotokolle dar. Eine Implementation muß zur Steuerung der zum IT-System gehörenden Teile ohnehin erfolgen. Durch Nutzung eines dadurch bereits vorhandenen Protokolls kann die Entwicklung und Implementation eines weiteren unterbleiben, was nach dem Prinzip des Minimalaufwandes das Produkt stabiler, einfacher und nicht zuletzt auch billiger macht. Dieses Prinzip wurde als fundamentales Axiom bei der Entwicklung von SNMP zugrundegelegt.

> Fundamental Axiom [Rose94]:
> The impact of adding network management to managed nodes must be minimal, reflecting a lowest common denominator.

Da die Managementprotokolle, speziell SNMP, allerdings für Aufgaben der Überwachung und Fehlermeldung entwickelt wurden, arbeiten sie teilweise verbindungslos, so daß keine gesicherte Datenübertragung gewährleistet ist. Auch die Möglichkeiten der Datenübertragung sind auf die im Managementbereich notwendigen Funktionen beschränkt. Bei der Kommunikation von Teilen eines computergestützten Managementsystems treten Kommunikationsanforderungen auf, die mittels solcher Protokolle nur mit zusätzlichen aufgepfropften Mechanismen erfüllt werden können. Damit funktioniert das System zwar, aber solche Anpassungen sind als suboptimal anzusehen. Besser ist ein auf die Anforderungen des Managementwerkzeuges angepaßtes Kommunikationsmodell.

Das Siemens-Produkt TransView setzt auf SNMP als zentrales Kommunikationsprotokoll.

4.2.3.2 CORBA

CORBA (Common Object Request Broker Architecture) kommt eine besondere Rolle zu, deshalb wird diesem Protokoll hier auch ein eigener Abschnitt gewidmet. Einzig das Produkt von IBM setzt auf dieser Architektur auf. Aufgrund seiner hohen Universalität ist eine Implementation sehr aufwendig und steht im Gegensatz zu dem im vorhergehenden Abschnitt erwähnten Axiom.

Die überragende Stärke dieser Architektur ist ihre beispielhafte Offenheit. Jedes beliebige Programm, welches CORBA implementiert, könnte theoretisch auf funktionaler Ebene in das Managementsystem integriert werden.

4.2.3.3 Proprietäre Ansätze

Da die Möglichkeiten der vorhandenen Managementprotokolle nicht ausreichten und die Verwirklichung einer eigenen CORBA-Implementation zu aufwendig schien, haben einige Hersteller proprietäre Protokolle entwickelt. CA‘s Unicenter TNG benutzt zur Kommunikation der Programmteile untereinander ein proprietäres Protokoll. Da jedoch alle diese Programmteile über Schnittstellen verfügen, können andere Hersteller an diese Schnittstellen andocken. Sie können lediglich nicht selbst als Agent auftreten. Auch OpenView benutzt zur Kommunikation innerhalb des Produktverbundes proprietäre Protokolle. Beide Produkte implementieren zusätzlich SNMP zur Kommunikation mit aktiven Netzwerkkomponenten.

4.2.4 Managementdatenbank

Die zugrundeliegende Datenbasis ist aufgrund der unterschiedlichen Herangehensweisen der einzelnen Anbieter naturgemäß verschieden. Der optimale Fall, ein einziges Repository für alle

Komponenten des IT-Systems zu implementieren, das sämtliche Informationen enthält, wird derzeit von keinem Produkt geboten. Für diese Anforderung wird man wohl noch bis zur Etablierung von WBEM warten müssen.

HP OpenView und SNI TransView haben für jede funktionale Einheit ihres Produktverbundes eine Datenbank. Bei einer Anfrage wird dann das jeweilige Produkt aktiv und liefert das gewünschte Datenmaterial zur Weiterverarbeitung an. Dadurch sind Informationen zu einer speziellen Komponente über mehrere Datenbanken verteilt, und eine Redundanz bestimmter Informationen ist nicht auszuschließen.

CA Unicenter TNG und Tivoli TME10 verfügen im Grundsatz über eine Datenbank, die alle angeschlossenen Programmteile mit Informationen versorgt. Durch die Integration von Fremdapplikationen, die nicht notwendigerweise auf Funktionsebene erfolgt, ergibt sich aber das Problem, daß diese ihre eigene Datenbank erstellen. In aller Regel ist eine übergreifende Nutzung speziell dieser Daten nicht möglich. Es gilt aber der Grundsatz, daß mit steigender Anzahl eigener Programmteile der Hersteller der Anteil der zentral vorgehaltenen Informationen zunimmt.

4.2.5 Vorverarbeitung von Ereignisdaten (Correlation)

Bei Auftreten eines Ereignisses irgendwo im IT-System kann es zu sogenannten Event-Storms kommen. Darunter versteht man eine große Menge von Ereignismeldungen, die alle durch ein einziges Ereignis verursacht werden. Dabei generiert jede Komponente des IT-Systems, die einen Service bereitstellt, welcher das fehlerhafte Element benutzt, ein Ereignis.

Die Herausforderung besteht nun darin, aus der Flut von Ereignissen dasjenige herauszugreifen, welches ursächlich für den Rest der Ereignisse war. Als Nebeneffekt kann die Identifikation der Ursache benutzt werden, um gleich automatische Aktionen zur Behebung des Problems einzuleiten.

Allgemein, d. h. bei Unicenter TNG, TME10 und TransView, wird ein regelbasiertes Korrelationssystem benutzt. HP geht mit OpenView einen anderen Weg. Hier kommt ein sogenannter `event correlation circuit` zum Einsatz, der in [She96] näher beschrieben wird.

Das Filtern von Ereignissen wird in den Produkten als Spezialfall der Ereigniskorrelation angesehen. Im Vergleich zur Identifikation des ursächlichen Ereignisses wirkt das Filtering geradezu trivial. Die Korrelationswerkzeuge können das Filtern der Ereignisse durch entsprechende Definition der Regeln bzw. der Objekte des Korrelationsplanes leisten. Meist gibt es technisch beschränkte Korrelationswerkzeuge als Filter für die Komponenten zum Ereignismanagement, welche keine Regeln zur Ereigniskorrelation akzeptieren. Die Funktionalität wird erst durch Zukauf der entsprechenden Lizenz erreicht.

4.2.6 Visualisierung der anfallenden Daten

Alle Systeme benutzen zur Darstellung der Daten ähnliche Verfahren. In der topologischen Ansicht wird über eine Signalisierung der Zustand der angezeigten Komponenten farbig dargestellt. In Abbildung 14 werden zwei verschiedene Zustandsinformationen an Teilen des IT-Systems signalisiert. Ein Gebäude hat eine Ausfallmeldung (dargestellt durch eine rote Markierung) und ein weiteres eine Warnmeldung (dargestellt durch eine gelbe Markierung). Beim Verfolgen des Problems findet man einen ausgefallenen Datenbankprozeß als Ursache heraus. Es wird also immer der kritischste Zustand propagiert. Je nach Interface unterscheidet sich die konkrete Darstellung etwas, das Prinzip bleibt aber stets gleich.

Die Ereigniskonsolen stellen alle aufgetretenen Ereignisse in Tabellenform dar, wobei es möglich ist, einen Eintrag auszuwählen, um detailliertere Informationen zu erhalten. Abbildung 15 zeigt ein Beispiel für die prinzipielle Anordnung von Ereignisdaten.

Auch andere Anzeigen wie Statistiken und Auslastungskurven sind über alle Produkte ähnlich aufgebaut. Zudem bieten alle Produkte

die Möglichkeit, die Anzeigen nach dem Geschmack des Benutzers zu definieren, so daß konkrete Unterschiede kaum auszumachen sind.

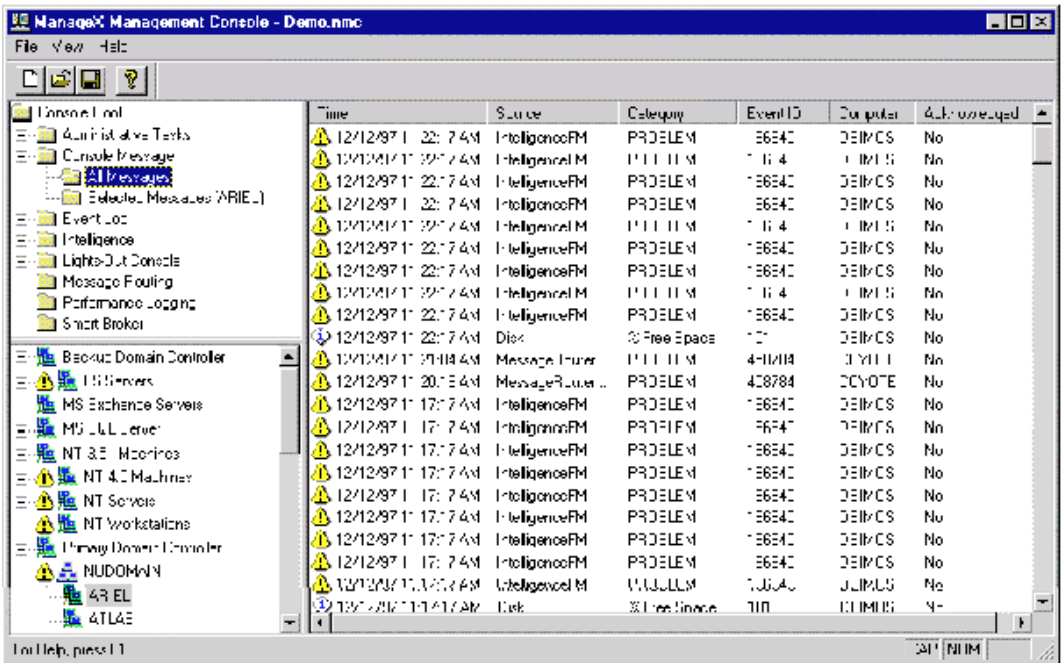

Abbildung 15: Event Konsole von HP ManageX als Beispiel für die Darstellung von Ereignissen

4.2.7 Client/Server-Ansatz

Alle in der Arbeit genannten Systeme arbeiten nach einem Client/Server-Modell. Dies ist insbesondere wichtig für eine Verteilung der Managementaufgaben. Leider ist, wie schon im Abschnitt 4.2.1 dargestellt, meist nur die Client-Applikation auf allen Plattformen implementiert. Für die Serveranwendungen wird in fast allen Fällen eine herstellerspezifische Plattform vorausgesetzt. Lediglich CA hat – weil kein Hardwarehersteller – auf den kleinsten gemeinsamen Nenner WindowsNT abgestellt.

Alle Produkte verfügen über einen Teil[28], der für die tatsächliche Verarbeitung der Daten verantwortlich ist. Um die Wege, die die Daten bis zur Verarbeitung zurücklegen müssen, kurz zu halten, ist es zweckmäßig, das Repository auf dieselbe Maschine zu implementieren. Das ist aber bei keinem der Produkte vorgeschrieben. Alle Produkte, die mit einem Repository arbeiten, also Unicenter TNG und TME 10, unterstützen auch die Verwendung von Datenbanken, die außerhalb der eigentlichen Managementanwendung liegen. Bei TransView und OpenView ist durch die andere Implementation (siehe Abschnitt 3.1) der Ort und die Art der Datenbank durch die jeweilige Funktionaleinheit bestimmt.

Daneben gibt es Module, die zur Kommunikation mit dem Benutzer des Systems dienen. Diese werden nur zur Datenvisualisierung oder Datenerfassung verwandt. Die Verarbeitung und Bereitstellung erfolgt am Server.

4.3 Organisatorische Anforderungen

Neben den technischen Anforderungen an ein System, die sich im allgemeinen auf eine möglichst breite Hardwareunterstützung und große Funktionsvielfalt reduzieren lassen, müssen organisatorische Belange des Unternehmens modellierbar sein. So müssen die Benutzer des Systems nach ihren Anforderungen an das System klassifiziert und entsprechende Veränderungen an den Interaktionsmöglichkeiten durchgeführt werden können. Das Managementsystem muß auch an die Struktur des IT-Systems angepaßt werden können.

4.3.1 Profilkonzept für Administratoren

Im Abschnitt 2.1.2.2 wurde kurz die Granulierung der Administrationsaufgaben angesprochen. Dies ist insbesondere bei personenbezogenen und anderen besonders zu schützenden Daten wichtig. So soll

[28] Wenn Serverinstanzen, wie im Abschnitt 4.3.2 beschrieben, eingesetzt werden, können es auch mehrere sein.

zwar der Administrator auf die Systeme z. B. der Personalabteilung vollen Zugriff erhalten, um den vereinbarten Service bereitzustellen, jedoch keinen Einblick in die Gehaltsdaten des gesamten Unternehmens bekommen. Um solche Anforderungen bei einem unternehmensweiten Managementsystem modellieren zu können, sind Profile für die Benutzer nötig. In diesen Profilen wird festgelegt, welche Informationen über das IT-System ein Benutzer sehen kann und welche er modifizieren darf. Um bei dem Beispiel zu bleiben, würde man ein eingeschränktes Administratorenprofil für Dienstleister erstellen, welches ihm Vollzugriff auf alle Systeme erlaubt, aber keinen Zugriff auf die Gehaltsdaten und deren Verzeichniseinträge.

Als Nebeneffekt dieser Profilverwaltung ist ein direktes Reporting möglich, indem Profile lediglich das Lesen von Informationen gestatten und über festgelegte Sichten auf das IT-System verfügen. Damit bleiben die Reports ständig aktuell, und es werden keine zusätzlichen Module zu deren Generierung benötigt.

Unicenter TNG hat die größten Schwächen im Hinblick auf die Durchgängigkeit des Profilkonzeptes. Dies liegt daran, daß unter WindowsNT die bereits angesprochenen Probleme bei der Strukturierung der Benutzer vorliegen. Unicenter setzt auf WindowsNT auf und verfügt damit nicht über Betriebssystemfunktionen, die die Benutzerverwaltung weitreichend unterstützen. Entsprechend fehlen im Produkt auch Funktionen zur Paßwortsynchronisation und unternehmensweiten Nutzerverwaltung, weil dies dem Neuimplementieren eines Verzeichnisdienstes für WindowsNT gleichgekommen wäre. Dieser Aufwand wurde nicht betrieben.

Die Produkte, deren Hauptkonsolen auf UNIX basieren, TME10, TransView und OpenView, bieten zumindest für Unix-basierte Systeme eine Benutzerverwaltung an, haben es damit aber auch einfacher, da die Authentifizierungsfunktionen dieser Betriebssysteme weit ausgereifter sind als die von WindowsNT. WindowsNT bleibt von diesen Funktionen ausgeschlossen, so daß eine komplette Behandlung des IT-Systems auch hier derzeit nicht möglich ist.

Alle Produkte sehen eine von der Nutzerverwaltung des Betriebssystems unabhängige Authentifizierung am Managementsystem vor; einerseits, weil die Benutzerverwaltung nicht für alle Plattformen verfügbar ist und dadurch eine Nutzung der originären Nutzerdaten nicht möglich ist, und andererseits, um durch die Administrationsprofile gleichzeitig ein Reporting am Managementsystem zu ermöglichen. Ein angemeldeter Benutzer kann sich während einer Sitzung am Betriebssystem mehrfach mit unterschiedlichen Namen am Managementsystem anmelden und damit gleichzeitig z. B. Management- und Reportingfunktionen nutzen.

Eine durchgängige Nutzerverwaltung mit Eintrag der Profile und Rechte am Managementsystem in die unternehmensweite Authentifizierungsstruktur erscheint zwar logischer und auch korrekter, die implementierte Lösung bietet jedoch auch Vorteile. Durch die Trennung der Authentifizierung von Betriebssystem und Managementsystem kann ein Benutzer unter seinem Namen mehrere Sichten auf das Managementsystem erhalten, ohne daß er mehrere Accounts benötigt. Wünschenswert wäre daher eine kombinierte Lösung, um die Vorteile beider Verwaltungsstrategien nutzen zu können.

4.3.2 Unterstützung von Managementserverinstanzen

Serverinstanzen werden benötigt, um die Menge der Daten überhaupt verarbeiten zu können und um die Netzlast gering zu halten.

Die einfachste Methode ist, nach einem Manager-of-Manager-Konzept Zwischenstationen zu generieren, die als Managementserver laufen und nur bestimmte Ereignisse an den übergeordneten Server weiterreichen. Dann sind die Forderungen nach lokaler Verarbeitung einerseits und Eskalation der Ereignisse andererseits automatisch erfüllt. Der Nachteil dieses Ansatzes liegt in der Statik des Konzeptes. Jede Serverinstanz hat eine begrenzte Menge an zu verwaltenden Objekten und ist auch nur innerhalb dieser Menge auskunftsfähig. Jede Anfrage, die über diese Menge hinausgeht, zieht Kommunikation mit mindestens einer anderen Serverinstanz nach sich. Vorteil dieses

Konzeptes ist die klare Aufteilung der Administrationsaufgaben, hohe Lokalität und geringe Belastung der einzelnen Instanzen bei entsprechendem Design der Struktur sowie einfache Konfigurierbarkeit und robuste Implementierbarkeit.

Abbildung 16 zeigt eine Prinzipstruktur eines solchen Systems. Das Zusammenspiel Agent / Managementsystem wird hierbei erweitert, indem Managementsysteme ihrerseits gegenüber der nächsthöheren Instanz wieder als Agent auftreten. Das Modell läßt sich beliebig erweitern, indem mehrere Server Teilaufgaben einer Konsole übernehmen. Das Prinzip bleibt aber stets das gleiche.

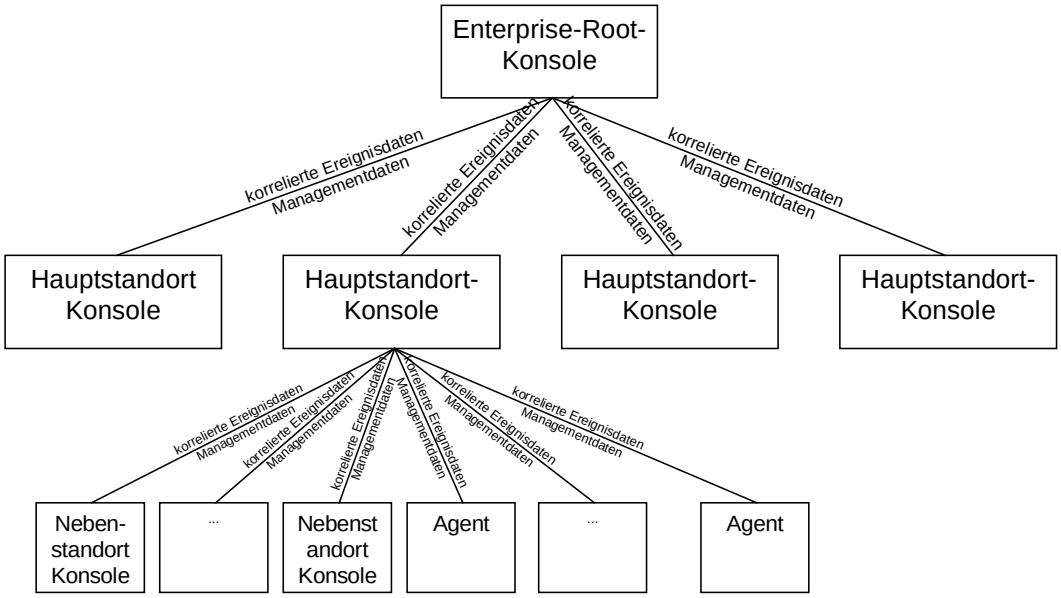

Abbildung 16: Hierarchische Managementinstanzen

Diese Vorgehensweise wird von allen vier Produkten unterstützt. Dazu müssen lediglich die Regeln im Ereignismanagement entsprechend definiert werden, so daß neben den Aktionen zur Behandlung des Ereignisses auch Ereignisse an die nächsthöhere Konsole gesendet werden. In jeder Serverinstanz liegt ein Repository vor, welches auch von anderen Serverinstanzen abgefragt und konfiguriert werden kann. Dazu ist nur eine Anmeldung am jeweiligen Server nötig. Ein automatisches Verfahren zum Abgleich der Repository oder automatisch

generierte Anfragen bei Zugriff auf ein entferntes Repository konnten bei keinem der Produkte gefunden werden.

Als Ausblick soll hier kurz erwähnt werden, daß in der neuen Version des Betriebssystems WindowsNT eine andere Form der Instanzierung vorgenommen wird. Es handelt sich dabei um eine Art Replikation der Verzeichniseinträge von einem Server zum nächsten [Kup98]. Dabei werden nicht alle Informationen repliziert, weil das zu einem hohen Synchronisationsaufwand führen würde. Statt dessen werden nur die häufig abgefragten Informationen repliziert. In der Folge verfügen alle Serverinstanzen über nahezu alle Informationen, die einem Teilnehmer des Serververbundes bekannt sind. Fehlt eine konkrete Information zu einem Objekt, wird sie automatisch beschafft und für eine gewisse Zeitspanne in einem Cache vorgehalten. Bei einer dynamischen Implementation könnte eine hohe Anzahl von Anfragen sogar dazu führen, daß sie dauerhaft repliziert wird.

Dieses Verfahren kann zwar nur durch einen ausgeklügelten Replikationsmechanismus funktionieren, stellt dann aber eine starke Weiterentwicklung gegenüber dem hierarchischen Modell dar. Insbesondere sind selbst bei Ausfall eines Servers nahezu alle Informationen weiter verfügbar. Allerdings plant Microsoft den Einsatz nur im Rahmen seines Active Directory Service, dessen Datenmengen bei weitem nicht so umfangreich sind, wie die eines Managementsystems.

5 Zusammenfassung

Die hohe Komplexität eines umfassenden Zugangs zum IT-System zeigt sich auch in der vorliegenden Arbeit. Die Konzeption ist stark vom konkreten System und dessen Anwendung abhängig. Deshalb sind allgemeingültige Implementationsanleitungen nicht möglich. Grundtendenzen können aber eingeschätzt werden. Zudem ist das Enterprise-IT-Management erst in den letzten beiden Jahren in das Interesse der Unternehmen gerückt, die sich Einsparungen durch Automatisierung von Administrationstätigkeiten versprechen. Und wirklich – warum soll ein IT-System nicht Benutzer und Administrator durch weitgehende Automatisierung entlasten?

In der heutigen IT-Administration werden nicht alle im zweiten Abschnitt angesprochenen Managementdisziplinen abgedeckt. Dies war anhand der im Verlauf dieser Arbeit besuchten Unternehmen festzustellen. Besonders den proaktiven Maßnahmen, der Dokumentation und den statistischen Auswertungen kommt heute wenig Bedeutung zu. Die Verwaltung erfolgt reaktiv, und der Zeitumfang der Mitarbeiter ist derartig bemessen, daß weitergehende Konzepte nur selten verfolgt werden können. Es werden also einerseits alle Aufgaben, die direkt mit dem Betrieb des IT-Systems in Zusammenhang stehen, mit aller Sorgfalt erledigt. Andererseits bleiben alle Tätigkeiten, die weniger praktische Relevanz haben, sondern mehr theoretischer, beobachtender Natur sind und für das Management nur mittelbar von Nutzen sein können, weitgehend außer Acht.

Die Administration erfolgt in mehr oder weniger stark differenzierten Abteilungen, wobei die Abteilungen der SBS Düsseldorf wenig gegliedert sind. Sie teilen die Aufgaben in nur drei Gruppen: Netzwerke, Systeme und Support. Diese intuitive Trennung führt zu Problemen. Hauptproblem ist die Kommunikation, die bei abteilungsübergreifenden Fehlern im IT-System entsteht.

Ein vorteilhafterer Ansatz ist demgegenüber die Behandlung des IT-Systems als Objekt, das in immer kleinere, unkompliziertere Funktionaleinheiten unterteilt wird. Dieses Ziel verfolgt das

Enterprise-IT-Management. Durch die Behandlung überschaubarer Funktionaleinheiten kann eine Person ein Problem eigenständig lösen. Der Kommunikationsaufwand verringert sich. Gleichzeitig kann die Teilung in First und Second Level Support erfolgen. Im First Level Support kommen Mitarbeiter zum Einsatz, die über ein breites Basiswissen verfügen und den großen Anteil von Standardproblemen direkt beheben. Im Second Level Support werden die Fachabteilungen mit Spezialisten angesiedelt. Diese Abteilungen lösen nur in Ausnahmefällen Probleme. Die Hauptaufgabe dieser Abteilungen besteht in der Planung und Realisierung der Fortentwicklung des IT-Systems, dessen Optimierung sowie der Modellierung und Dokumentation in den Managementwerkzeugen. Da die Problemlösung dem First Level Support obliegt, steht die dazu benötigte Zeit eher zur Verfügung als bei herkömmlichen Verwaltungsmodellen.

Die Sicht auf das Objekt IT-System und deren konsequente Anwendung führen zur Erhöhung der Verfügbarkeit, Sicherheit und Flexibilität des IT-Systems. Erkauft werden diese Vorteile durch drastisch erhöhten Modellierungsaufwand. Auch in Hardware und Software müssen Investitionen getätigt werden.

Die derzeit verfügbaren Produkte sind noch nicht völlig ausgereift und daraus resultieren Schwierigkeiten beim Einsatz und bei der Anpassung an das Unternehmen. Aus Gegebenheiten des Marktes und ihrer geschichtlichen Entwicklung heraus besitzen sie hauptsächlich Schwächen hinsichtlich der Konsequenz des Verwaltungsansatzes und der Unterstützung verschiedener Plattformen. Dadurch erhöht sich der Wartungsaufwand. Die Entwicklung schreitet jedoch schnell fort, so daß mit einer immer besseren Unterstützung der einzelnen Managementdisziplinen zu rechnen ist. Da in den letzten Jahren die Kosten zur Unterhaltung eines IT-Systems (TCO[29]) in den Vordergrund rückten, gibt es zahlreiche Initiativen, die die Weiterentwicklung von Hard- und Software zur besseren Unterstützung des IT-Managements vorantreiben.

[29] TCO – Total Cost of Ownership

Die Verwaltung von IT-Systemen ist stark von der Trennung in Netzwerke und Systeme geprägt. Das ist eine logische Folge ihrer Entwicklung aus UNIX- oder hostbasierten Systemen. Durch die langjährige Erfahrung in dieser Form der Verwaltung und die starke Belastung der Mitarbeiter im täglichen Betrieb des Systems wird selten der Ansatz der Verwaltung in Frage gestellt. Mit dem beschriebenen Enterprise-IT-Management können Vorteile erzielt werden, wenn dem Unternehmen der Mut zur Innovation nicht fehlt. Diese Arbeit soll als Denkanstoß für die Verwalter von IT-Systemen zum Ändern des Verwaltungsansatzes dienen – dem ersten Schritt zur Optimierung des IT-Managements.

References

[BMC1] BMC Corporate Staff. (1999). *BMC Software Inc*. Available: http://www.bmc.com. (Accessed 01/03/99).

[Brü98] Helmut Brühl, Heinz-Willi Schaefer. (1998, 10/05/1998). (Interview: Patrick Agsten). SBS GmbH & Co. OHG Düsseldorf.

[CeBIT5] o. V. (1998). Zentral alles im Griff. *CeBIT spezial, 05,* 9.

[CMU1] Jeffrey D. Case, Mark Fedor, Martin Lee Schoffstall, James R. Davin. (1990). *A Simple Network Management Protocol (SNMP)* [RFC 1157]. Carnegie Mellon University (36).
Keith McCloghrie. (1996). *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)* [RFC 1902]. Carnegie Mellon University (40).

[CMU2] Andy Bierman, Robin Iddon. (1997). *Remote Network Monitoring MIB Protocol Identifiers* [RFC 2074]. Carnegie Mellon University (43).

[CMU3] Steven Waldbusser. (1995). *Remote Network Monitoring Information Base* [RFC 1757]. Carnegie Mellon University (91).

[CMU4] Marshal T. Rose, Keith McCloghrie. (1991). *Concise MIB Definitions* [RFC 1212]. Carnegie Mellon University (19).
Keith McCloghrie, Marshal T. Rose. (1991). *Management Information Base for Network Management of TCP/IP-based internets: MIB-II* [RFC 1213]. Carnegie Mellon University (70).

[Die95] Norbert Diehl. (1995). *Mobile Computing: Systeme, Kommunikation, Anwendungen.* Bonn u.a.: Thomson.

[Durr91] Michael Durr, Mark Gibbs. (1991). *Praxis der PC-Vernetzung: Hard- und Software, Administration, Sicherheitsfragen.* Bonn u.a.: Addison-Wesley.

[Fit92] Trevor Fitchett. (1992). *Network Management.* London: British Standards Institution.

[Frey98] Gundolf S. Freyermuth. (1998). Computer machen Leute. *c't Magazin für Computertechnik, 04,* 90-97.

[Geb96] Jochen Gebauer. (1996). *Microsoft Systems Management Server 1.x.* Bonn: Addison-Wesley.

[Gie98] Kerstin Gießner. (1998, 30/06/1998). (Interview: Patrick Agsten). HP GmbH Leipzig.

[Gro98] Armin Groß. (1998, 23/09/1998). (Interview: Patrick Agsten). CA GmbH Darmstadt.

[Hab98] Gerhard Haberstroh. (1998, 17/09/1998). (Interview: Patrick Agsten). GUUG-Tagung Wiesbaden.

[Held92] Gilbert Held. (1992). *Network Management: Techniques, Tools and Systems.* Chichester u.a.: John Wiley & Sons.

[HSM1] Manfred Zörnpfennig. (1997, 02/02). *POLYCENTER Hierarchical Storage Management (HSM) for OpenVMS*. Available: http://www.digital.at/diginew/DECPRODUKTE/SysMan/pchierarchie.htm (Accessed 19/10/98).

[Hus91] Donna S. Hussain, Khateeb M. Hussain. (1991). *Information Systems for Business.* New York u.a.: Prentice Hall.

[ISO1] ISO JTC1. (1992). *ISO/IEC 10040* [Systems management overview]. Information technology -- Open Systems Interconnection. Genf: ISO/IEC.

[ISO2] ISO JTC1. (1989). *ISO/IEC 7498* [Basic Reference Model]. Information technology -- Open System Interconnection. Genf: ISO/IEC.
ISO JTC1. (1991). *ISO/IEC 9595* [Common management information service definition]. Information technology -- Open System Interconnection. Genf: ISO/IEC.
ISO JTC1. (1991). *ISO/IEC 9596* [Common management information protocol]. Information technology -- Open System Interconnection. Genf: ISO/IEC.
ISO JTC1. (1992). *ISO/IEC 10040* [Systems management overview]. Information technology -- Open Systems Interconnection. Genf: ISO/IEC.
ISO JTC1. (1988). *ISO/IEC 8571* [File Transfer, Access and Management]. Information Processing Systems -- Open System Interconnection. Genf: ISO/IEC.
ISO JTC1. (1990). *ISO/IEC 9594* [The Directory]. Information Processing Systems -- Open System Interconnection. Genf: ISO/IEC.

[ISO3] ISO JTC1. (1991). *ISO/IEC 9596* [Common management information protocol]. Information technology -- Open System Interconnection. Genf: ISO/IEC.

[ISO4] ISO JTC1. (1989). *ISO/IEC 7498* [Basic Reference Model]. Information technology -- Open System Interconnection. Genf: ISO/IEC.

[ISO5] ISO JTC1. (1992). *ISO/IEC 10165* [Management Information Services]. Information technology -- Open System Interconnection. Genf: ISO/IEC.

[Koch97] Olaf Koch. (1997). *WindowsNT 4 Server - Das Kompendium*. Haar bei München: Markt und Technik, Buch und Softwareverlag.

[Kor97] Rolf Kornemann. (1997, 24/06/97). (Interview: Patrick Agsten). Universität Leipzig.

[Kro94] David M. Kroenke, Richard Hatch. (1994). *Management Information Systems*. New York u.a.: McGraw Hill Text.

[Ku7-98] Jürgen Kuri. (1998). Artisten im Netz, ratlos. *c't Magazin für Computertechnik, 07,* 188-195.

[Ku13-98] Jürgen Kuri. (1998). PC am Draht - Wired for Management: PC-Verwaltung ganz einfach. *c't Magazin für Computertechnik, 13*, 146-152.

[Kup98] Martin Kuppinger. (1998). Aktiv Dienst. *Windows Guide, 4,* 82-87.

[Leb98] Horst Leber. (1998, 17/09). *Unicenter TNG*. GUUG-Tagung. Wiesbaden.

[MW1] o.V. (1997). *Merriam-Webster's Collegiate Dictionary* (10th). Brittanica CD 97.

[OV1] HP Corporate Staff. (1997). *HP OpenView IT/Administration: Integrated Network and Systems Management.* o.O.: HP.

[Rem1] Remedy Corporate Staff. (1998). *Adaptable Enterprise Applications – Remedy Corporation*. Available: http://www.remedy.com. (Accessed 01/03/98).

[Rose94] Marshal T. Rose. (1994). *The Simple Book: An Introduction to Internet Management.* Englewood Cliffs: Prentice Hall.

[Rum91] James Rumbaugh, Michael Blaha, William Premerlani, Frederick Eddi, William Lorensen. (1991). *Object-Oriented Modeling And Design.* New York: Prentice Hall.

[She96] Kenneth R. Sheers. (1996). HP OpenView Event Correlation Services. *Hewlett-Packard Journal, 10.*

[Shn93] Ben Shneiderman. (1993). *Designing the user interface: Strategies for effective human-computer interaction.* Reading, MS.: Addison-Wesley.

[Spec1] Cabletron Corporate Staff. (1998). SPECTRUM Family of Management Products. Available: http://www.Cabletron.com/spectrum. (Accessed 06/03/98).

[TNG1] CA Corporate Staff. (1997). *Unicenter TNG - Management der Unternehmens-DV*. o.O.

[TNG2] CA Corporate Staff. (1998). Unicenter TNG. Available: http://www.cai.com/products/unicent/framework/tng_framework_overview.htm. (Accessed 06/03/98).

[TNG3] CA Corporate Staff. (1997). *Unicenter TNG Administrator Guide*. Unicenter Framework CD.

[TNG4] CA Corporate Staff. (1996). *TNGDEMO*.

[TME1] Rolf Lendenmann u.a. (1998). Understanding Tivoli's TME 3.0 and TME 10. Available: http://www.tivoli.com/redbooks. (Accessed 10/04/98).

[TV1] SNI Corporate Staff. (1998). *TransView - Konzepte, Lösungen*. o.O.: SNI.

[WBEM1] o.V. (1998). Web-Based Enterprise Management. Available: http://wbem.freerange.com/wbem/standards.htm. (Accessed 21/10/1998).

[WBEM2] Microsoft Corporate Staff. (1998). WBEM Schema Home Page. Available: http://www.microsoft.com/management/wbem/default.htm. (Accessed 21/10/1998).

[WBEM3] Microsoft Corporate Staff. (1998, 05/06). *WBEM CIM Schema v1*. Available: http://www.microsoft.com/management/wbem/contents/CIM_schema_v1.htm. (Accessed 28/09/98).

Eidesstattliche Erklärung

Ich versichere, daß ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Leipzig	07. 04. 1999	
Ort	Datum	Unterschrift